CCNP Security
FIREWALL 642-618
Official Cert Guide

David Hucaby
Dave Garneau
Anthony Sequeira

Cisco Press
800 East 96th Street
Indianapolis, IN 46240
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 LTM’s) 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

Introduction xxv

Chapter 1 Cisco ASA Adaptive Security Appliance Overview 3
Chapter 2 Working with a Cisco ASA 35
Chapter 3 Configuring ASA Interfaces 75
Chapter 4 Configuring IP Connectivity 113
Chapter 5 Managing a Cisco ASA 161
Chapter 6 Recording ASA Activity 243
Chapter 7 Using Address Translation 279
Chapter 8 Controlling Access Through the ASA 391
Chapter 9 Inspecting Traffic 473
Chapter 10 Using Proxy Services to Control Access 583
Chapter 11 Handling Traffic 607
Chapter 12 Using Transparent Firewall Mode 629
Chapter 13 Creating Virtual Firewalls on the ASA 651
Chapter 14 Deploying High Availability Features 671
Chapter 15 Integrating ASA Service Modules 715
Chapter 16 Traffic Analysis Tools 729
Chapter 17 Final Preparation 765

Appendix A Answers to the “Do I Know This Already?” Quizzes 771
Appendix B CCNP Security 642-618 FIREWALL Exam Updates: Version 1.0 777

Glossary of Key Terms 779

Index 789
Contents

Introduction xxv

Chapter 1Cisco ASA Adaptive Security Appliance Overview 3

“Do I Know This Already?” Quiz 3

Foundation Topics 7

Firewall Overview 7

Firewall Techniques 11

Stateless Packet Filtering 11

Stateful Packet Filtering 12

Stateful Packet Filtering with Application Inspection and Control 12

Network Intrusion Prevention System 13

Network Behavior Analysis 14

Application Layer Gateway (Proxy) 14

Cisco ASA Features 15

Selecting a Cisco ASA Model 18

ASA 5505 18

ASA 5510, 5520, and 5540 19

ASA 5550 20

ASA 5580 21

Security Services Modules 22

Advanced Inspection and Prevention (AIP) SSM 22

Content Security and Control (CSC) SSM 23

4-port Gigabit Ethernet (4GE) SSM 24

ASA 5585-X 24

ASA Performance Breakdown 25

Selecting ASA Licenses 29

ASA Memory Requirements 31

Exam Preparation Tasks 33

Review All Key Topics 33

Define Key Terms 33

Chapter 2Working with a Cisco ASA 35

“Do I Know This Already?” Quiz 35

Foundation Topics 40

Using the CLI 40

Entering Commands 41

Command Help 43

Searching and Filtering Command Output 45
Managing Software and Feature Activation  
Managing Cisco ASA Software and ASDM Images  
Upgrading Files from a Local PC or Directly from Cisco.com  
Considerations When Upgrading from OS Version 8.2 to 8.3 or Higher  
License Management  
Upgrading the Image and Activation Key at the Same Time  
Cisco ASA Software and License Verification  
Configuring Management Access  
Overview of Basic Procedures  
Configuring Remote Management Access  
Configuring an Out-of-Band Management Interface  
Configuring Remote Access Using Telnet  
Configuring Remote Access Using SSH  
Configuring Remote Access Using HTTPS  
Creating a Permanent Self-Signed Certificate  
Obtaining an Identity Certificate by PKI Enrollment  
Deploying an Identity Certificate  
Configuring Management Access Banners  
Controlling Management Access with AAA  
Creating Users in the Local Database  
Using Simple Password-Only Authentication  
Configuring AAA Access Using the Local Database  
Configuring AAA Access Using Remote AAA Server(s)  
Step 1: Create a AAA Server Group and Configure How Servers in the Group Are Accessed  
Step 2: Populate the Server Group with Member Servers  
Step 3: Enable User Authentication for Each Remote Management Access Channel  
Configuring Cisco Secure ACS for Remote Authentication
Improper Translation 337
Protocols Incompatible with NAT or PAT 337
Proxy ARP 338
NAT-Related Syslog Messages 338
Implementing NAT in ASA Software Versions 8.3 and Later 339
Major Differences in NAT Beginning in Software Version 8.3 339
Network Objects 339
NAT Control 340
Integrating NAT with Other ASA Functions 340
NAT “Direction” 340
NAT Rule Priority 340
New NAT Options in OS Versions 8.3 and Later 340
NAT Table 341
Configuring Auto (Object) NAT 343
Configuring Static Translations Using Auto NAT 344
Configuring Static Port Translations Using Auto NAT 349
Comparing Static NAT Configurations from OS Versions 8.2 and 8.3 351
Configuring Dynamic Translations Using Auto NAT 352
Using Object Groups in NAT Rules 357
Comparing Dynamic NAT Configurations from OS Versions 8.2 and 8.3 360
Verifying Auto (Object) NAT 361
Configuring Manual NAT 363
Examining the Syntax of the Manual NAT Command 368
Configuring a NAT Exemption Using Manual NAT 369
Configuring Twice NAT 370
Configuring Translations Using Manual NAT After Auto NAT 374
Configuring a Unidirectional Manual Static NAT Rule 376
Inserting a Manual NAT Rule in a Specific Location 378
Comparing Manual NAT Configurations from OS versions 8.2 and 8.3 379
When Not to Use NAT 381
Tuning NAT 381
Troubleshooting NAT 383
Improper Translation 383
Proxy ARP and Syslog Messages 385
Egress Interface Selection 385
Exam Preparation Tasks 386
Review All Key Topics 386
Define Key Terms 387
Command Reference to Check Your Memory 387

Chapter 8 Controlling Access Through the ASA 391
“Do I Know This Already?” Quiz 392
Foundation Topics 397
Understanding How Access Control Works 397
State Tables 397
Connection Table 398
TCP Connection Flags 401
Inside and Outside, Inbound and Outbound 403
Local Host Table 403
State Table Logging 405
Understanding Interface Access Rules 405
Stateful Filtering 406
Interface Access Rules and Interface Security Levels 408
Interface Access Rules Direction 408
Default Access Rules 410
The Global ACL 411
Configuring Interface Access Rules 412
Access Rule Logging 417
Configuring the Global ACL 421
Cisco ASDM Public Server Wizard 424
Configuring Access Control Lists from the CLI 425
Implementation Guidelines 426
Time-Based Access Rules 427
Configuring Time Ranges from the CLI 432
Verifying Interface Access Rules 432
Managing Rules in Cisco ASDM 434
Managing Access Rules from the CLI 437
Organizing Access Rules Using Object Groups 438
Verifying Object Groups 439
Configuring and Verifying Other Basic Access Controls 454
Shunning 455
Troubleshooting Basic Access Control 457
Examining Syslog Messages 457
Packet Capture 459
Packet Tracer 460
Chapter 9 Inspecting Traffic 473

“Do I Know This Already?” Quiz 473

Foundation Topics 479

Understanding the Modular Policy Framework 479

Configuring the MPF 482

Configuring a Policy for Inspecting OSI Layers 3 and 4 484

Step 1: Define a Layers 3–4 Class Map 484
Step 2: Define a Layers 3–4 Policy Map 486
Step 3: Apply the Policy Map to the Appropriate Interfaces 490
Creating a Security Policy in ASDM 490
Tuning Basic Layers 3–4 Connection Limits 495
Inspecting TCP Parameters with the TCP Normalizer 499
Configuring ICMP Inspection 505

Configuring Dynamic Protocol Inspection 507
Configuring Custom Protocol Inspection 514

Configuring a Policy for Inspecting OSI Layers 5–7 517

Configuring HTTP Inspection 518
Configuring HTTP Inspection Policy Maps
   Using the CLI 519
Configuring HTTP Inspection Policy Maps
   Using ASDM 527

Configuring FTP Inspection 539
Configuring FTP Inspection Using the CLI 540
Configuring FTP Inspection Using ASDM 542

Configuring DNS Inspection 546
Creating and Applying a DNS Inspection Policy Map
   Using the CLI 546
Creating and Applying a DNS Inspection Policy Map
   Using ASDM 549

Configuring ESMTP Inspection 552
Configuring an ESMTP Inspection with the CLI 553
Configuring an ESMTP Inspection with ASDM 556

Configuring a Policy for ASA Management Traffic 559

Detecting and Filtering Botnet Traffic 561
Configuring Botnet Traffic Filtering with ASDM 564
Step 1: Configure the Dynamic Database 565
Step 2: Configure the Static Database 565
Step 3: Enable DNS Snooping 566
Step 4: Enable the Botnet Traffic Filter 566
Configuring Botnet Traffic Filtering with the CLI 568
Step 1: Configure the Dynamic Database 568
Step 2: Configure the Static Database 568
Step 3: Enable DNS Snooping 568
Step 4: Enable the Botnet Traffic Filter 569
Using Threat Detection 570
Configuring Threat Detection in ASDM 571
Step 1: Configure Basic Threat Detection 571
Step 2: Configure Advanced Threat Detection 571
Step 3: Configure Scanning Threat Detection 572
Configuring Threat Detection with the CLI 572
Step 1: Configure Basic Threat Detection 573
Step 2: Configure Advanced Threat Detection 576
Step 3: Configure Scanning Threat Detection 577
Exam Preparation Tasks 579
Review All Key Topics 579
Define Key Terms 580
Command Reference to Check Your Memory 580

Chapter 10 Using Proxy Services to Control Access 583
“Do I Know This Already?” Quiz 583
Foundation Topics 586
User-Based (Cut-Through) Proxy Overview 586
User Authentication 586
User Authentication and Access Control 587
Implementation Examples 587
AAA on the ASA 587
AAA Deployment Options 587
User-Based Proxy Preconfiguration Steps and Deployment Guidelines 588
User-Based Proxy Preconfiguration Steps 588
User-Based Proxy Deployment Guidelines 589
Direct HTTP Authentication with the Cisco ASA 589
Chapter 14 Deploying High Availability Features 671

“Do I Know This Already?” Quiz 671

Foundation Topics 675

ASA Failover Overview 675
  Failover Roles 675
  Detecting an ASA Failure 681

Configuring Active-Standby Failover Mode 683
  Configuring Active-Standby Failover with the ASDM Wizard 683
  Configuring Active-Standby Failover Manually in ASDM 687
  Configuring Active-Standby Failover with the CLI 689
  Step 1: Configure the Primary Failover Unit 689
  Step 2: Configure Failover on the Secondary Device 690

Configuring Active-Active Failover Mode 692
  Configuring Active-Active Failover in ASDM 692
  Configuring Active-Active Failover with the CLI 696
  Step 1: Configure the Primary ASA Unit 696
  Step 2: Configure the Secondary ASA Unit 697

Tuning Failover Operation 701
  Configuring Failover Timers 701
  Configuring Failover Health Monitoring 702
  Detecting Asymmetric Routing 703
  Administering Failover 705

Verifying Failover Operation 706

Leveraging Failover for a Zero Downtime Upgrade 708

Exam Preparation Tasks 710
Chapter 15  **Integrating ASA Service Modules**  715

“Do I Know This Already?” Quiz  715

Foundation Topics  718

Cisco ASA Security Services Modules Overview  718

Module Components  718

*General Deployment Guidelines*  719

*Overview of the Cisco ASA Content Security and Control SSM*  719

*Cisco Content Security and Control SSM Licensing*  720

*Overview of the Cisco ASA Advanced Inspection and Prevention SSM and SSC*  720

*Inline Operation*  720

*Promiscuous Operation*  721

*Supported Cisco IPS Software Features*  721

Installing the ASA AIP-SSM and AIP-SSC  721

The Cisco AIP-SSM and AIP-SSC Ethernet Connections  722

Failure Management Modes  722

Managing Basic Features  722

Initializing the AIP-SSM and AIP-SSC  723

Configuring the AIP-SSM and AIP-SSC  723

Integrating the ASA CSC-SSM  724

Installing the CSC-SSM  724

Ethernet Connections  724

Managing the Basic Features  724

Initializing the Cisco CSC-SSM  725

Configuring the CSC-SSM  725

Exam Preparation Tasks  726

Review All Key Topics  726

Define Key Terms  726

Command Reference to Check Your Memory  726

Chapter 16  **Traffic Analysis Tools**  729

“How Do I Know This Already?” Quiz  729

Foundation Topics  733

Testing Network Connectivity  733

Using Packet Tracer  737
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>
<thead>
<tr>
<th>Exam Topic</th>
<th>Chapter Where Topic Is Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASA Basic Configurations</td>
<td></td>
</tr>
<tr>
<td>Identify the ASA product family</td>
<td>Chapters 1, 15</td>
</tr>
<tr>
<td>Implement ASA licensing</td>
<td>Chapter 1</td>
</tr>
<tr>
<td>Manage the ASA boot process</td>
<td>Chapter 2</td>
</tr>
<tr>
<td>Implement ASA interface settings</td>
<td>Chapters 3, 8</td>
</tr>
<tr>
<td>Implement ASA management features</td>
<td>Chapters 2, 4, 5, 6, 16</td>
</tr>
<tr>
<td>Implement ASA access control features</td>
<td>Chapters 8, 10</td>
</tr>
<tr>
<td>Implement NAT on the ASA</td>
<td>Chapter 7</td>
</tr>
<tr>
<td>Implement ASDM public server feature</td>
<td>Chapter 2</td>
</tr>
<tr>
<td>Implement ASA QoS settings</td>
<td>Chapter 11</td>
</tr>
<tr>
<td>Implement ASA transparent firewall</td>
<td>Chapter 12</td>
</tr>
<tr>
<td>ASA Routing Features</td>
<td></td>
</tr>
<tr>
<td>Implement ASA static routing</td>
<td>Chapter 4</td>
</tr>
<tr>
<td>Implement ASA dynamic routing</td>
<td>Chapter 4</td>
</tr>
<tr>
<td>ASA Inspection Policy</td>
<td></td>
</tr>
<tr>
<td>Implement ASA inspections features</td>
<td>Chapter 9</td>
</tr>
<tr>
<td>ASA Advanced Network Protections</td>
<td></td>
</tr>
<tr>
<td>Implement ASA botnet traffic filter</td>
<td>Chapter 9</td>
</tr>
<tr>
<td>ASA High Availability</td>
<td></td>
</tr>
<tr>
<td>Implement ASA interface redundancy and</td>
<td>Chapter 3</td>
</tr>
<tr>
<td>load sharing features</td>
<td></td>
</tr>
<tr>
<td>Implement ASA virtualization feature</td>
<td>Chapter 13</td>
</tr>
<tr>
<td>Implement ASA stateful failover</td>
<td>Chapter 14</td>
</tr>
</tbody>
</table>
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:

- **Configuring Physical Interfaces:** This section discusses Cisco ASA interfaces that can be connected to a network through physical cabling, as well as the parameters that determine how the interfaces will operate.

- **Configuring VLAN Interfaces:** This section covers logical interfaces that can be used to connect an ASA to VLANs over a trunk link.

- **Configuring Interface Security Parameters:** This section explains the parameters you can set to assign a name, an IP address, and a security level to an ASA interface.

- **Configuring the Interface MTU:** This section discusses the maximum transmission unit size and how it can be adjusted to set the largest possible Ethernet frame that can be transmitted on an Ethernet-based ASA interface.

- **Verifying Interface Operation:** This section covers the commands you can use to display information about ASA interfaces and confirm whether they are operating as expected.
A Cisco Adaptive Security Appliance (ASA) must be configured with enough information to begin accepting and forwarding traffic before it can begin doing its job of securing networks. Each of its interfaces must be configured to interoperate with other network equipment and to participate in the IP protocol suite. This chapter discusses each of these topics in detail.

“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 3-1 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>
<thead>
<tr>
<th>Foundation Topics Section</th>
<th>Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring Physical Interfaces</td>
<td>1–4</td>
</tr>
<tr>
<td>Configuring VLAN Interfaces</td>
<td>5–7</td>
</tr>
<tr>
<td>Configuring Interface Security Parameters</td>
<td>8–10</td>
</tr>
<tr>
<td>Configuring the Interface MTU</td>
<td>11</td>
</tr>
<tr>
<td>Verifying Interface Operation</td>
<td>12</td>
</tr>
</tbody>
</table>

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 this 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 answers describe an attribute of a redundant interface?  
   (Choose all that apply.)
   a. A redundant interface load balances traffic across member interfaces.
   b. A redundant interface is made up of two or more physical interfaces.
   c. An ASA can have up to eight redundant interface pairs.
   d. Each member interface of a redundant interface cannot have its own security level.
   e. IP addresses must be applied to the member physical interfaces of a redundant interface.
   f. The member interfaces swap the active role when one of them fails.

2. What must happen for a member interface to take over the active role as part of a redundant interface?
   a. Three hello messages must be missed.
   b. The link status of the current active interface goes down.
   c. A member interface, which was previously active before it went down, regains its link status.
   d. Its member priority is higher than other member interfaces.
   e. A timer must expire.

3. Which ASA command can be used to display a list of all physical interfaces?
   a. show interfaces physical
   b. show interface list
   c. show hardware
   d. show version
   e. show ports
   f. show

4. Suppose you want to double the bandwidth between an ASA's outside interface and a neighboring switch. A single GigabitEthernet link exists today; a second link would also add redundancy. Which one of the following describes the best approach to meet the requirements?
   a. Bring up a second GigabitEthernet interface on the same VLAN as the first one.
   b. Configure the two interfaces as a redundant interface.
   c. Configure the two interfaces as an EtherChannel.
   d. Dual links are not possible on an ASA.
5. You have been assigned the task of configuring a VLAN interface on an ASA 5510. The interface will use VLAN 50. Which one of the following sets of commands should be entered first to accomplish the task?

- a. `interface vlan 50
   no shutdown`
- b. `interface ethernet0/0
   no shutdown`
- c. `interface ethernet0/0.5
   vlan 50
   no shutdown`
- d. `interface ethernet0/0.50
   no shutdown`

6. Which of the following are correct attributes of an ASA interface that is configured to support VLAN interfaces? (Choose all that apply.)

- a. The physical interface operates as an ISL trunk.
- b. The physical interface operates as an 802.1Q trunk.
- c. The subinterface numbers of the physical interface must match the VLAN number.
- d. All packets sent from a subinterface are tagged for the trunk link.
- e. An ASA can negotiate a trunk link with a connected switch.

7. Which one of the following answers contains the commands that should be entered on an ASA 5505 to create an interface for VLAN 6?

- a. `interface vlan 6`
- b. `vlan 6`
- c. `interface ethernet0/0.6`
- d. `interface ethernet0/0.6`

8. Which of the following represent security attributes that must be assigned to an active ASA interface when the ASA is in routed firewall mode? (Choose three answers.)

- a. IP address
- b. Access list
- c. Interface name
- d. Security level
- e. Interface priority
- f. MAC address
9. Which one of the following interfaces should normally be assigned a security level value of 100?
   a. outside  
   b. dmz  
   c. inside  
   d. None of these answers are correct.

10. An ASA has two active interfaces, one with security level 0 and one with security level 100. Which one of the following statements is true?
   a. Traffic is permitted to be initiated from security level 0 toward security level 100.  
   b. Traffic is permitted to be initiated from security level 100 toward security level 0.  
   c. Traffic is not permitted in either direction.  
   d. The interfaces must have the same security level by default before traffic can flow.

11. Suppose you are asked to adjust the MTU on the “inside” ASA interface Ethernet0/1 to 1460 bytes. Which one of the following answers contains the correct command(s) to enter?
   a. ciscoasa(config)# mtu 1460  
   b. ciscoasa(config)# mtu inside 1460  
   c. ciscoasa(config)# interface ethernet0/1  
      ciscoasa(config-if)# mtu 1460  
   d. None of these answers are correct; the MTU must be greater than 1500.
12. From the following output, which of the following statements are true about ASA interface Ethernet0/2? (Choose all that apply)

```bash
ciscoasa# show nameif
Interface Name Security
Ethernet0/0 outside 0
Ethernet0/1 inside 100
Management0/0 management 100
ciscoasa#
ciscoasa# show interface ethernet0/2
Interface Ethernet0/2 ,, is administratively down, line protocol is down
Hardware is i82546GB rev03, BW 100 Mbps, DLY 100 usec
    Auto-Duplex, Auto-Speed
    Input flow control is unsupported, output flow control is unsupported
    Available but not configured via nameif
    MAC address 001a.a22d.1dde, MTU not set
    IP address 10.1.1.1, subnet mask 255.255.255.0
0 packets input, 0 bytes, 0 no buffer
0 received broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 pause input, 0 resume input
0 L2 decode drops
0 packets output, 0 bytes, 0 underruns
0 pause output, 0 resume output
0 output errors, 0 collisions, 1 interface resets
0 late collisions, 0 deferred
0 input reset drops, 0 output reset drops, 0 tx hangs
input queue (blocks free curr/low): hardware (255/255)
output queue (blocks free curr/low): hardware (255/255)
ciscoasa#
```

- **a.** The interface is configured and is live on the network.
- **b.** The interface is not ready to use; the `no shutdown` command has not been issued.
- **c.** The interface is not ready to use; it doesn't have an IP address configured.
- **d.** The interface is not ready to use; it doesn't have a MAC address configured.
- **e.** The interface is not ready to use; it doesn't have a security level configured.
- **f.** The interface is not ready to use; it doesn't have an interface name configured.

Answer E might also be true, but you cannot confirm that a security level has been configured from the command output given. Because an interface name has not been configured with the `nameif` command, neither the interface name nor the security level is shown in the output.
Foundation Topics

Every ASA has one or more interfaces that can be used to connect to some other part of the network so that traffic can be inspected and controlled. ASA interfaces can be physical, where actual network media cables connect, or logical, where the interfaces exist internally and are passed to the network over a physical link. In this chapter, you learn how to configure both types of interfaces for connectivity and IP addressing.

In addition, to pass and inspect traffic, each interface must be configured with the following three security attributes:

- Interface name
- IP address and subnet mask
- Security level

You learn how to configure the security parameters in the section, “Configuring Interface Security Parameters.”

Configuring Physical Interfaces

An ASA supports multiple physical interfaces that can be connected into the network or to individual devices. From the Configuration tab in Cisco ASDM, you can view the list of interfaces by selecting Device Setup > Interfaces, as shown in Figure 3-1.

![Figure 3-1 Using ASDM to View a List of Interfaces](image)
From the CLI, you can see a list of the physical firewall interfaces that are available by using the following command:

ciscoasa# show version

Firewall interfaces are referenced by their hardware index and their physical interface names. Example 3-1 lists the physical interfaces in an ASA 5510. Ethernet0/0 through 0/3 and Management0/0 are built-in interfaces, while GigabitEthernet1/0 through 1/3 are installed as a 4GE-SSM module.

**Example 3-1  Listing Physical ASA Interfaces**

<table>
<thead>
<tr>
<th>Interface</th>
<th>Type</th>
<th>Address</th>
<th>IRQ</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet0/0</td>
<td>Ext:</td>
<td>001a.a22d.1ddc</td>
<td>9</td>
</tr>
<tr>
<td>Ethernet0/1</td>
<td>Ext:</td>
<td>001a.a22d.1ddd</td>
<td>9</td>
</tr>
<tr>
<td>Ethernet0/2</td>
<td>Ext:</td>
<td>001a.a22d.1dde</td>
<td>9</td>
</tr>
<tr>
<td>Ethernet0/3</td>
<td>Ext:</td>
<td>001a.a22d.1ddf</td>
<td>9</td>
</tr>
<tr>
<td>Management0/0</td>
<td>Ext:</td>
<td>001a.a22d.1ddbb</td>
<td>11</td>
</tr>
<tr>
<td>Internal-Data0/0</td>
<td>Int:</td>
<td>0000.0001.0002</td>
<td>11</td>
</tr>
<tr>
<td>Not used</td>
<td>Int:</td>
<td></td>
<td>5</td>
</tr>
<tr>
<td>GigabitEthernet1/0</td>
<td>Ext:</td>
<td>001a.a22d.20f1</td>
<td>255</td>
</tr>
<tr>
<td>GigabitEthernet1/1</td>
<td>Ext:</td>
<td>001a.a22d.20f2</td>
<td>255</td>
</tr>
<tr>
<td>GigabitEthernet1/2</td>
<td>Ext:</td>
<td>001a.a22d.20f3</td>
<td>255</td>
</tr>
<tr>
<td>GigabitEthernet1/3</td>
<td>Ext:</td>
<td>001a.a22d.20f4</td>
<td>255</td>
</tr>
<tr>
<td>Internal-Data1/0</td>
<td>Int:</td>
<td></td>
<td>255</td>
</tr>
</tbody>
</table>

Licensed features for this platform:

Maximum Physical Interfaces : Unlimited
Before you begin configuring the ASA interfaces, you should first use the interface list to identify each of the interfaces you will use. At a minimum, you need one interface as the “inside” of the ASA and one as the “outside.”

Default Interface Configuration

Some interfaces come predefined in the initial factory default configuration. You can view the interface mappings with the `show nameif` EXEC command. As shown in Example 3-2, an ASA 5510 or higher model defines only one interface, Management0/0, for use by default. The interface is named “management” and is set aside for out-of-band management access.

Example 3-2  Default Interface Configuration on ASA 5510 and Higher Models

```
ciscoasa# show nameif
Interface                Name                     Security
Management0/0            management               100
```

An ASA 5505 takes a different approach with its default interfaces, as shown in Example 3-3. Rather than use physical interfaces, it defines an “inside” and an “outside” interface using two logical VLANs: VLAN 1 and VLAN 2.

Example 3-3  Default Interface Configuration on the ASA 5505

```
ciscoasa# show nameif
Interface                Name                     Security
Vlan1                    inside                    100
Vlan2                    outside                    0
```

These two VLANs are then applied to the physical interfaces such that interface Ethernet0/0 is mapped to VLAN 2, while Ethernet0/1 through 0/7 are mapped to VLAN 1 (inside). This configuration gives one outside interface that can be connected to a service provider network for an Internet connection. The remaining seven inside interfaces can be connected to individual devices on the protected network.

You can display the ASA 5505 interface-to-VLAN mapping by entering the `show switch vlan` command, as shown in Example 3-4.
Example 3-4  Displaying the ASA 5505 Interface-to-VLAN Mapping

<table>
<thead>
<tr>
<th>VLAN Name</th>
<th>Status</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>inside</td>
<td>up</td>
<td>Et0/1, Et0/2, Et0/3, Et0/4, Et0/5, Et0/6, Et0/7</td>
</tr>
<tr>
<td>outside</td>
<td>up</td>
<td>Et0/0</td>
</tr>
</tbody>
</table>

ciscoasa#

Configuring Physical Interface Parameters

For each physical interface, you can configure the speed, duplex, and the interface state. In ASDM, select Configuration > Interfaces, select an interface, and click the Edit button. In the General tab, click Configure Hardware Properties, as shown in Figure 3-2.

You can do the same task from the CLI by using the following commands:

ciscoasa(config)# interface hardware-id

ciscoasa(config-if)# speed {auto | 10 | 100 | 1000}

ciscoasa(config-if)# duplex {auto | full | half}

ciscoasa(config-if)# [no] shutdown
By default, an interface uses autodetected speed and autonegotiated duplex mode, as if the `speed auto` and `duplex auto` commands had been entered. As long as the ASA interface and the device connected to it are configured the same, the interface will automatically come up using the maximum speed and full-duplex mode. You can also statically configure the interface speed to 10, 100, or 1000 Mbps, as well as full or half duplex mode.

By default, physical interfaces are administratively shut down. Use the `no shutdown` interface configuration command to enable each one individually. As well, you can shut an interface back down with the `shutdown` command.

**Note:** Other parameters, such as the interface name, security level, and IP address, should be configured, too. These are discussed in the section, “Configuring Interface Security Parameters.”

### Mapping ASA 5505 Interfaces to VLANs

By default, an ASA 5505 maps interface Ethernet0/0 to VLAN 2 and interfaces Ethernet0/1 through 0/7 to VLAN 1. All eight interfaces are connected to an internal 8-port switch, with each interface configured as an access link mapped to a single VLAN.

Figure 3-3 shows how ASDM can be used to map a physical interface to a different VLAN number. First, a new interface is created and named vlan 10. At the top of the Add Interface dialog box, Ethernet0/3 is added to the list of interfaces that are mapped to VLAN 10.

You can use the following CLI command to accomplish the same task:

```
ciscoasa(config-if)# switchport access vlan vlan-id
```

The `vlan-id` parameter represents a VLAN interface that has already been created and configured. The section, “Configuring VLAN Interfaces,” covers this in detail.

In Example 3-5, interface Ethernet0/3 is mapped to VLAN 10, while Ethernet0/4 is mapped to VLAN 20.

**Example 3-5  Mapping Interfaces to VLANs on an ASA 5505**

```
ciscoasa(config)# interface ethernet0/3
ciscoasa(config-if)# switchport access vlan 10
```

```
ciscoasa(config-if)# interface ethernet0/4
```

```
ciscoasa(config-if)# switchport access vlan 20
```

### Configuring Interface Redundancy

By default, each physical ASA interface operates independently of any other interface. The interface can be in one of two operating states: up or down. When an interface is down for some reason, the ASA cannot send or receive any data through it. For example,
the switch port where an ASA interface connects might fail, causing the ASA interface to go down, too.

To keep an ASA interface up and active all the time, you can configure physical interfaces as redundant pairs. As a redundant pair, two interfaces are set aside for the same ASA function (inside, outside, and so on), and connect to the same network. Only one of the interfaces is active at any given time; the other interface stays in a standby state. As soon as the active interface loses its link status and goes down, the standby interface becomes active and takes over passing traffic.

Both physical interfaces in a redundant pair are configured as members of a single logical “redundant” interface. To join two interfaces as a redundant pair, the interfaces must be of the same type (10/100/1000BASE-TX, for example).

The redundant interface, rather than its physical member interfaces, is configured with a unique interface name, security level, and IP address—all the parameters used in ASA interface operations.
First, you must create the redundant interface by entering the following configuration command:

```plaintext
ciscoasa(config)# interface redundant number
```

You can define up to eight redundant interfaces on an ASA. Therefore, the interface number can be 1 through 8.

Next, use the following command to add a physical interface as a member of the redundant interface:

```plaintext
ciscoasa(config-int)# member-interface physical_interface
```

Here, `physical_interface` is the hardware name and number, like ethernet0/1 or giga-bitethernet0/1, for example. In Figure 3-4, ASA interfaces Ethernet0/0 and Ethernet0/1 are member interfaces of a logical redundant interface called Redundant1, while Ethernet0/2 and Ethernet0/3 are members of interface Redundant2.

![Figure 3-4 Example Redundant Interfaces](image)

Be aware that the member interface cannot have a security level or an IP address configured. In fact, as soon as you enter the `member-interface` command, the ASA will automatically clear those parameters from the physical interface configuration. You should repeat this command to add a second physical interface to the redundant pair.

Keep in mind that the order in which you configure the interfaces is important. The first physical interface added to a logical redundant interface will become the active interface. That interface will stay active until it loses its link status, causing the second or standby interface to take over. The standby interface can also take over when the active interface is administratively shut down with the `shutdown` interface configuration command.

However, the active status will not revert to the failed interface, even when it comes back up. The two interfaces trade the active role back and forth only when one of them fails.

The redundant interface also takes on the MAC address of the first member interface that you configure. Regardless of which physical interface is active, that same MAC address will be used. You can override this behavior by manually configuring a unique MAC address on the redundant interface with the `mac-address mac_address` interface configuration command.

In Example 3-6, interfaces Ethernet0/0 and Ethernet0/1 are configured to be used as logical interface redundant 1.
Example 3-6  Configuring a Redundant Interface Pair

```cisco
Example 3-6  Configuring a Redundant Interface Pair

ciscoasa(config)# interface redundant 1
ciscoasa(config-if)# member-interface ethernet0/0
INFO: security-level and IP address are cleared on Ethernet0/0.
ciscoasa(config-if)# member-interface ethernet0/1
INFO: security-level and IP address are cleared on Ethernet0/1.
ciscoasa(config-if)# no shutdown
```

The redundant interface is now ready to be configured as a normal ASA interface. From this point on, you should not configure anything on the two physical interfaces other than the port speed and duplex.

**Note:** Make sure the logical redundant interface and the two physical interfaces are enabled with the `no shutdown` command. Even though they are all logically associated, they can be manually shut down or brought up independently.

To accomplish the same thing through ASDM, first select **Add > Redundant Interface** from the drop-down menu in the upper-right corner of the interface listing. A new Add Redundant Interface dialog box appears, as shown in Figure 3-5. Select the redundant interface number and the two physical interfaces that will operate as a redundant pair. To enable the new redundant interface for use, be sure to check the **Enable Interface** check box.

**Note:** Other parameters, such as the interface name, security level, and IP address, should be configured, too. These are discussed in the section, “Configuring Interface Security Parameters.”

### Configuring an EtherChannel

A single link between an ASA and a switch provides simple connectivity, but it is a single point of failure. If the link goes down, no data can travel across it. In the previous section, you learned that a redundant interface binds two physical interfaces into one logical interface. The possibility of a link failure is reduced, because one of the two interfaces will always be up and available; however, only one of the two links can pass data at any given time.

How can you maximize availability with more than one link, while leveraging the bandwidth of all of them at the same time? Beginning with ASA software release 8.4(1), you can use an EtherChannel to make that all possible. With an EtherChannel, two to eight active physical interfaces can be grouped or bundled together as a single logical port-channel interface. Each interface must be of the same type, speed, and duplex mode before an EtherChannel can be built.

Figure 3-6 shows an EtherChannel that is built out of multiple physical GigabitEthernet interfaces that connect an ASA to a Catalyst switch. On the ASA, the resulting logical interface is named interface port-channel 1. Notice that the individual links in the EtherChannel can have different interface names on each end. The interfaces can also be
connected and grouped in any arbitrary order. What matters is that the interfaces form one common EtherChannel link between the two devices.

**Figure 3-5**  Adding a Redundant Interface in ASDM

**Figure 3-6**  Building an EtherChannel from Multiple Physical Links
An ASA can support up to eight active interfaces in a single EtherChannel; however, you can configure up to 16 different interfaces per EtherChannel, although only eight of them can be active at any time. If one active interface fails, another one automatically takes its place. Although Figure 3-6 shows a single EtherChannel link, an ASA can support up to 48 different EtherChannels.

Because multiple interfaces are active in an EtherChannel, the available bandwidth can be scaled over that of a single interface. Traffic is load balanced by distributing the packets across the active interfaces. The ASA computes a hash value based on values found in the packet header, such as the source or destination MAC address, IP address, or the UDP or TCP port number. You can configure a preset combination of fields that are used. As long as the number of active interfaces is a multiple of two, the ASA can evenly distribute packets across them.

To build an EtherChannel, the ASA and the switch must both agree to do so. You can configure the ASA interfaces to statically participate, where the EtherChannel is “always on.” In that case, the switch interfaces must also be configured for “always on” operation. Instead, you can configure the ASA and switch to negotiate an EtherChannel with each other.

Negotiation uses the Link Aggregation Control Protocol (LACP), which is a standards-based protocol. LACP packets are exchanged between the ASA and the switch over the interfaces that can become part of an EtherChannel. The ASA and the switch use a system priority (a 2-byte priority value followed by a 6-byte switch MAC address) to decide which one is allowed to make decisions about what interfaces are actively participating in the EtherChannel at a given time.

Interfaces are selected and become active according to their port priority value (a 2-byte priority followed by a 2-byte port number), where a low value indicates a higher priority. A set of up to 16 potential links can be defined for each EtherChannel. Through LACP, up to eight of these having the lowest port priorities can become active EtherChannel links at any given time. The other links are placed in a standby state and will be enabled in the EtherChannel if one of the active links goes down.

LACP can be configured in the active mode, in which the ASA actively asks a far-end switch to negotiate an EtherChannel, or in passive mode, in which the ASA negotiates an EtherChannel only if the far end initiates it. Table 3-2 summarizes the EtherChannel negotiation methods and characteristics.

### Table 3-2 EtherChannel Negotiation Methods

<table>
<thead>
<tr>
<th>Negotiation Mode</th>
<th>Negotiation Packets Sent?</th>
<th>Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>On</td>
<td>No</td>
<td>All ports channeling all the time</td>
</tr>
<tr>
<td>Passive</td>
<td>Yes</td>
<td>Waits to channel until asked</td>
</tr>
<tr>
<td>Active</td>
<td>Yes</td>
<td>Actively asks to form a channel</td>
</tr>
</tbody>
</table>

To configure an EtherChannel in ASDM, begin by defining the port-channel interface. Select **Configuration > Device Setup > Interfaces**, click the **Add** button, and select...
**EtherChannel Interface.** Under the General tab, enter an arbitrary Port Channel ID number (1 to 48) that will identify the port-channel interface.

Next, select an interface from the Available Physical Interface list and click the Add button to make it a member of the EtherChannel. You can repeat this process to add multiple interfaces. Make sure to select the Enable Interface check box to enable the port-channel interface for use. In Figure 3-7, interface port-channel1 has been created. Ethernet0/2 and Ethernet0/3 have been added as member interfaces.

![Figure 3-7 Configuring a New EtherChannel in ASDM](image)

**Note:** Before an interface can be configured for an EtherChannel, it must not have a name configured. After the EtherChannel interfaces are configured, you can define a name and other security parameters on the port-channel interface.

Notice that Figure 3-7 also has fields for Interface Name, Security Level, and IP Address. These fields are not applied to the individual member interfaces; instead, they are applied to the port-channel interface. The fields are covered in the section, “Configuring Interface Security Parameters.”

Next, configure the method that the ASA will use to distribute packets across the links within the EtherChannel. By default, a packet’s source and destination IP addresses are used to compute a hash index that points to the link that will carry the packet. This is the appropriate choice in most cases, as long as the source and destination IP addresses are
unique and diverse. The more varied the hash input values, the better the traffic will be distributed across the links in the EtherChannel.

In some scenarios, the majority of the traffic might travel between the same two IP addresses, causing most of the packets to travel over only one link of the EtherChannel. In that case, you can configure the EtherChannel load-balancing method to use additional information, such as a Layer 4 port number, MAC addresses, or a VLAN number, to provide more uniqueness so that the packets can be spread more evenly across the EtherChannel links. The possible load-balancing methods are as follows:

- Destination IP
- Destination IP and Layer 4 Port
- Destination MAC Address
- Destination Layer 4 Port
- Source and Destination IP Address
- Source and Destination MAC Address
- Source and Destination IP Address and Layer 4 Port
- Source and Destination Layer 4 Port
- Source IP Address
- Source IP Address and Layer 4 Port
- Source MAC Address
- Source Layer 4 Port
- VLAN Destination IP Address
- VLAN Destination IP and Layer 4 Port
- VLAN Only
- VLAN Source and Destination IP Address
- VLAN Source and Destination IP Address and Layer 4 Port
- VLAN Source IP Address
- VLAN Source IP Address and Layer 4 Port

To configure the load-balancing method, select the Advanced tab in the Add EtherChannel Interface screen and choose the method from the drop-down list at the bottom of the screen, as shown in Figure 3-8.

Next, you need to configure a negotiation method for the EtherChannel. ASDM uses a default method of “active” on each member interface, where the ASA will use LACP to actively ask the far-end switch to bring up the EtherChannel. To configure the method, select Configuration > Device Setup > Interfaces, select an interface that is a member of the EtherChannel, and click the Edit button. In Figure 3-9, interfaces Ethernet0/2 and 0/3
are shown to be members of the Port-channel1 group. Because their individual configurations are restricted, they are shown with a lock icon next to their names. Remember that the security parameters of an EtherChannel are configured on the Port-channel interface instead.

![Figure 3-8 Configuring the EtherChannel Load-Balancing Method](image)

Under the General tab of the Edit Interface screen, make sure that the Enable Interface check box under the Channel Group is selected. Select the Advanced tab and use the EtherChannel drop-down menu to set the negotiation mode, which can be either Active, Passive, or On, as shown in Figure 3-10.

You can configure more interfaces in the channel group number than are allowed to be active in the channel. This prepares extra standby interfaces to replace failed active ones. Set a lower LACP port priority (1 to 65,535; default 32,768) for any interfaces that must be active and a higher priority for interfaces that might be held in the standby state. Otherwise, just use the default scenario, in which all ports default to 32,768, and the lower port numbers (in interface number order) are used to select the active ports.

By default, an ASA uses LACP system priority of 32,768. If the ASA and the switch both use the same value, the one with the lower MAC address becomes the decision maker over the LACP negotiations. You can change the system priority by selecting Configuration > Device Setup > EtherChannel.
Chapter 3: Configuring ASA Interfaces

Figure 3-9  Selecting an EtherChannel Interface for Configuration

Figure 3-10  Configuring the EtherChannel Negotiation Method
You can also configure an EtherChannel by using the CLI. Select a physical interface that will be a member of the EtherChannel, and then identify the port-channel number where it will belong, along with the negotiation method that will be used:

```plaintext
ciscoasa(config)# lacp system-priority priority
ciscoasa(config)# interface type mod/num
ciscoasa(config-if)# channel-protocol lacp
ciscoasa(config-if)# channel-group number mode {on | passive | active}
ciscoasa(config-if)# lacp port-priority priority
```

As an example of LACP configuration, suppose that you want to configure an ASA to actively negotiate an EtherChannel using interfaces Ethernet0/2 and 0/3. You can use the commands listed in Example 3-7 to accomplish this.

**Example 3-7  Configuring an EtherChannel Using the CLI**

```plaintext
CISCOASA(config)# interface ethernet0/2
CISCOASA(config-if)# channel-protocol lacp
CISCOASA(config-if)# channel-group 1 mode active
CISCOASA(config-if)# exit
CISCOASA(config)# interface ethernet0/3
CISCOASA(config-if)# channel-protocol lacp
CISCOASA(config-if)# channel-group 1 mode active
CISCOASA(config-if)# exit
```

If you find that an EtherChannel is having problems, remember that the entire concept is based on consistent configurations on both ends of the channel. You can verify the EtherChannel state with the `show port-channel summary` command. Each port in the channel is shown, along with flags indicating the port's state, as shown in Example 3-8.

**Example 3-8  show port-channel summary Command Output**

```plaintext
CISCOASA# show port-channel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        U - in use      N - not in use, no aggregation/nameif
        M - not in use, no aggregation due to minimum links not met
        w - waiting to be aggregated
Number of channel-groups in use: 1
Group  Port-channel  Protocol    Ports
      +------------------------------+
      1     Po1(U)            LACP    Et0/2(P)   Et0/3(P)
CISCOASA#
```

The status of the port channel shows the EtherChannel logical interface as a whole. This should show U (in use) if the channel is operational. You also can examine the status of
each interface within the channel. Notice that both of the channel interfaces have flags (P), which indicate that they are active in the port-channel.

**Configuring VLAN Interfaces**

A physical ASA interface can be configured to connect to multiple logical networks. To do this, the interface is configured to operate as a VLAN trunk link. On ASA 5510 and higher platforms, each VLAN that is carried over the trunk link terminates on a unique subinterface of a physical interface. On an ASA 5505, each VLAN is defined by a unique VLAN interface and can connect to physical interfaces and be carried over a VLAN trunk link.

**VLAN Interfaces and Trunks on ASA 5510 and Higher Platforms**

An ASA trunk link supports only the IEEE 802.1Q trunk encapsulation method. As each packet is sent over a trunk link, it is tagged with its source VLAN number. As packets are removed from the trunk, the tag is examined and removed so that the packets can be forwarded to their appropriate VLANs. Figure 3-11 shows how a trunk link between an ASA and a switch can encapsulate or carry frames from multiple VLANs.

![Figure 3-11 IEEE 802.1Q Trunk Link Operation with an ASA](image)

IEEE 802.1Q trunk links support the concept of a native VLAN. Frames coming from the native VLAN are sent over the trunk link without a tag, while frames from other VLANs have a tag added while in the trunk. By default, only packets that are sent out the ASA's physical interface itself are not tagged, and they appear to use the trunk's native VLAN. Packets that are sent out a subinterface do receive a VLAN tag.

**Note:** Although a Cisco switch can be configured to negotiate the trunk status or encapsulation through the Dynamic Trunking Protocol (DTP), ASA platforms cannot. Therefore, an ASA trunk link is either on or off, according to the subinterface configuration. You should make sure that the switch port is configured to trunk unconditionally, too.
You can configure a trunk link by using the following configuration commands:

```cisco
CiscoASA(config)# interface hardware_id.subinterface
CiscoASA(config-subif)# vlan vlan_id
```

First, use the `interface` command to identify the physical interface that will become a trunk link and the subinterface that will be associated with a VLAN number. The physical interface is given as `hardware_id`, such as Ethernet0/3, followed by a dot or period. A subinterface number is added to the physical interface name to create the logical VLAN interface. This is an arbitrary number that must be unique for each logical interface.

Use the `vlan vlan_id` subinterface configuration command to specify the VLAN number. The subinterface number does not have to match the VLAN number, although it can for convenience and readability.

As an example, Figure 3-12 shows a network diagram of a trunk link between an ASA and a switch. ASA physical interface Ethernet0/3 is used as the trunk link. VLAN 10 is carried over ASA subinterface Ethernet0/3.1, while VLAN 20 is carried over Ethernet0/3.2. The trunk link can be configured with the commands listed in Example 3-9.

![Figure 3-12 Network Diagram for Example 3-9 Trunk Link Configuration](image)

**Example 3-9 Configuring a Trunk Link on an ASA**

```cisco
CiscoASA(config)# interface ethernet0/3
CiscoASA(config-if)# no shutdown
CiscoASA(config-if)# interface ethernet0/3.1
CiscoASA(config-subif)# vlan 10
CiscoASA(config-subif)# no shutdown
CiscoASA(config-subif)# interface ethernet0/3.2
CiscoASA(config-subif)# vlan 20
CiscoASA(config-subif)# no shutdown
```

The same trunk link configuration can be accomplished with ASDM. Subinterfaces used in a trunk link must first be added or created. In the interface list view, select the Add > Interface function in the upper-right corner of the ASDM application. Select the hardware port or physical interface that will be used for the trunk link. In Figure 3-13, Ethernet0/3 is used. Because subinterface Ethernet0/3.1 is being created, the subinterface ID is set to 1. The VLAN ID is set to 10.
Note: Other parameters, such as the interface name, security level, and IP address, should be configured, too. These are discussed in the section, “Configuring Interface Security Parameters.”

### VLAN Interfaces and Trunks on an ASA 5505

On an ASA 5505, VLANs are supported on the physical interfaces, but only if corresponding logical VLAN interfaces are configured. For example, if VLAN 1 is to be used, the `interface vlan 1` command must be entered to create the internal VLAN and the VLAN interface.

By default, the ASA 5505 platform includes the `interface vlan 1` and `interface vlan 2` commands in its configuration.
Other parameters, such as the interface name, security level, and IP address, should be configured on VLAN interfaces rather than on physical interfaces. These are discussed in the section, “Configuring Interface Security Parameters.”

If you need to carry multiple VLANs over a link to a neighboring switch, you can configure an ASA 5505 physical interface as a VLAN trunk link. First, create the individual VLANs with the `interface vlan` configuration command. Then, configure the physical interface to operate in IEEE 802.1Q trunk mode and allow specific VLANs to be carried over it with the following interface configuration commands:

```cisco
switchport mode trunk
switchport trunk allowed vlan vlan-list
```

By default, no VLANs are permitted to be carried over a trunk link. You must identify which VLANs can be carried by entering `vlan-list`, which is a comma-separated list of VLAN numbers. In Example 3-10, an ASA 5505 is configured to support VLANs 10 and 20 and carry those VLANs over interface Ethernet0/5, which is configured as a trunk link.

**Example 3-10  ASA VLAN CLI Configuration**

```cisco
interface vlan 10
exit
interface vlan 20
exit
interface ethernet0/5
switchport mode trunk
switchport trunk allowed vlan 10,20
```

### Configuring Interface Security Parameters

Once you identify an ASA interface that will be connected to the network, you will need to apply the following three security parameters to it:

- **Interface name**
- **IP address**
- **Security level**

These parameters are explained in the following sections.

### Naming the Interface

ASA interfaces are known by two different names:

- **Hardware name**: Specifies the interface type, hardware module, and port number. The hardware names of physical interfaces can include Ethernet0/0, Management0/0, and GigabitEthernet1/0. Hardware names of VLAN interfaces have a subinterface suffix, such as Ethernet0/0.1. Hardware names are predefined and cannot be changed.

- **Interface name**: Specifies the function of the interface, relative to its security posture. For example, an interface that faces the outside, untrusted world might be
named “outside,” whereas an interface that faces the inside, trusted network might be
to an ASA interface, you must first enter the interface configura-
To assign an interface name to an ASA interface, you must first enter the interface configu-
An ASA uses the interface name when
security policies are applied.

ciscoasa(config-if)# nameif if_name

In Example 3-11, interface Ethernet0/0 is configured with the interface name “outside.”

Example 3-11  Assigning an Interface Name

ciscoasa(config)# interface ethernet0/0
ciscoasa(config-if)# nameif outside

You can set the interface name in ASDM by editing an existing interface or adding a new

Assigning an IP Address

To communicate with other devices on a network, an ASA interface needs its own IP ad-
This mode is covered in Chapter 12, “Using Transparent Firewall Mode.”

You can use the following interface configuration command to assign a static IP address
If you omit the subnet-mask parameter, the firewall assumes that a classful network (Class
If you use subnetting in your network, be sure to specify the correct subnet mask rather
that the firewall derives from the IP address.

Continuing the process from Example 3-9, so that the outside interface is assigned IP ad-
Continuing the process from Example 3-9, so that the outside interface is assigned IP ad-

If the ASA is connected to a network that offers dynamic IP address assignment, you
should not configure a static IP address on the interface. Instead, you can configure the
ASA to request an IP address through DHCP or PPPoE. Only DHCP is covered in the
FIREWALL course and exam.

You can use the following interface configuration command to force the interface to re-
quest its IP address from a DHCP server:

ciscoasa(config-if)# ip address dhcp [setroute]
Adding the `setroute` keyword causes the ASA to set its default route automatically, based on the default gateway parameter that is returned in the DHCP reply. This is handy because the default route should always correlate with the IP address that is given to the interface. If the `setroute` keyword is not entered, you will have to explicitly configure a default route.

Once the ASA obtains an IP address for the interface via DHCP, you can release and renew the DHCP lease by re-entering the `ip address dhcp` command.

You can set a static interface IP address in ASDM by editing an existing interface or adding a new one. First, select Use Static IP in the IP Address section, as shown previously in Figure 3-13, and then enter the IP address. For the subnet mask, you can type in a mask or select one from a drop-down menu.

If the interface requests an IP address through DHCP, select the Obtain Address via DHCP option. By default, the ASA will use the interface MAC address in the DHCP request. To get a default gateway automatically through DHCP, check the Obtain Default Route Through DHCP check box. You can click the Renew DHCP Lease button at any time to release and renew the DHCP lease.

**Setting the Security Level**

ASA platforms have some inherent security policies that are based on the relative trust or security level that has been assigned to each interface. Interfaces with a higher security level are considered to be more trusted than interfaces with a lower security level. The security levels can range from 0 (the least amount of trust) to 100 (the greatest amount of trust).

Usually, the “outside” interface that faces a public, untrusted network should receive security level 0. The “inside” interface that faces the community of trusted users should receive security level 100. Any other ASA interfaces that connect to other areas of the network should receive a security level between 1 and 99. Figure 3-14 shows a typical scenario with an ASA and three interfaces.

By default, interface security levels must be unique so that the ASA can apply security policies across security-level boundaries. This is because of the two following inherent policies that an ASA uses to forward traffic between its interfaces:

- Traffic is allowed to flow from a higher-security interface to a lower-security interface (inside to outside, for example), provided that any access list, stateful inspection, and address translation requirements are met.

- Traffic from a lower-security interface to a higher one cannot pass unless additional explicit inspection and filtering checks are passed.

This concept is shown in Figure 3-15, applied to an ASA with only two interfaces.

In addition, the same two security policies apply to any number of interfaces. Figure 3-16 shows an ASA with three different interfaces and how traffic is inherently permitted to flow from higher-security interfaces toward lower-security interfaces. For example, traffic coming from the inside network (security level 100) can flow toward the DMZ network (security level 50) because the security levels are decreasing. As well, DMZ traffic (security level 50) can flow toward the outside network (security level 0).
Chapter 3: Configuring ASA Interfaces

**Figure 3-14**  *Example ASA with Interface Names and Unique Security Levels*

**Figure 3-15**  *Inherent Security Policies Between ASA Interfaces*

**Figure 3-16**  *Traffic Flows Are Permitted from Higher to Lower Security Levels*
Traffic that is initiated in the opposite direction, from a lower security level toward a higher one, cannot pass so easily. Figure 3-17 shows the same ASA with three interfaces and the possible traffic flow patterns.

You can assign a security level of 0 to 100 to an ASA interface with the following interface configuration command:

```
ciscoasa(config-if)# security-level level
```

From ASDM, you can set the security level when you edit an existing interface or add a new one.

Continuing from the configuration in the section, “Assigning an IP Address,” you can assign the outside interface with a security level of 0 by entering the following:

```
ciscoasa(config-if)# security-level 0
```

By default, interface security levels do not have to be unique on an ASA. However, if two interfaces have the same security level, the default security policy will not permit any traffic to pass between the two interfaces at all. You can override this behavior with the `same-security-traffic permit inter-interface` command.

In addition, there are two cases in which it is not possible to assign unique security levels to each ASA interface:

- **The number of ASA interfaces is greater than the number of unique security level values:** Because the security level can range from 0 to 100, there are 101 unique values. Some ASA platforms can support more than 101 VLAN interfaces, so it becomes impossible to give them all unique security levels. In this case, you can use the following command in global configuration mode so that you can reuse security level numbers and relax the security level constraint between interfaces, as shown in the left portion of Figure 3-18:

```
ciscoasa(config)# same-security-traffic permit inter-interface
```
Figure 3-18  Permitting Traffic to Flow Across the Same Security Levels

- **Traffic must enter and exit through the same interface, traversing the same security level:** When an ASA is configured to support logical VPN connections, multiple connections might terminate on the same ASA interface. This VPN architecture looks much like the spokes of a wheel, where the ASA interface is at the hub or center. When traffic comes from one VPN spoke and enters another spoke, it essentially enters the ASA interface and comes out of one VPN connection, only to enter a different VPN connection and go back out the same interface. In effect, the VPN traffic follows a hairpin turn on a single interface.

If an ASA is configured for VPN connections, you can use the following command in global configuration mode to relax the security level constraint within an interface, as shown in the right portion of Figure 3-18:

ciscoasa(config)# same-security-traffic permit intra-interface

If you are using ASDM, you can accomplish the same tasks from the **Configuration > Device Setup > Interfaces** using the two check boxes at the bottom of the interface list, as illustrated in Figure 3-19.

**Interface Security Parameters Example**

The ASA in Figure 3-14 has three interfaces. Example 3-12 shows the commands that can be used to configure each of the interfaces with the necessary security parameters.

**Example 3-12  Configuring the ASA Interfaces from Figure 3-14**

```
ciscoasa(config)# interface ethernet0/0
ciscoasa(config-if)# nameif outside

ciscoasa(config-if)# ip address 192.168.254.2 255.255.255.0

ciscoasa(config-if)# security-level 0

ciscoasa(config-if)# interface ethernet0/1

ciscoasa(config-if)# nameif inside

ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0

ciscoasa(config-if)# security-level 100

ciscoasa(config-if)# interface ethernet0/2

ciscoasa(config-if)# nameif dmz

ciscoasa(config-if)# ip address 192.168.100.1 255.255.255.0

ciscoasa(config-if)# security-level 50
```
Configuring the Interface MTU

By default, any Ethernet interface has its maximum transmission unit (MTU) size set to 1500 bytes, which is the maximum and expected value for Ethernet frames. If a packet is larger than the MTU, it must be fragmented before being transmitted. And before the packet can be presented at the destination, all of its fragments must be reassembled in their proper order.

The whole fragmentation and reassembly process takes time, memory, and CPU resources, so it should be avoided if possible. Normally, the default 1500-byte MTU is sufficient because Ethernet frames are limited to a standard maximum of 1500 bytes of payload data. Various IEEE standards use expanded frame sizes to carry additional information. As well, data centers often leverage Ethernet “giant” or “jumbo” frames, which are much larger than normal, to move large amounts of data efficiently.

If packets larger than 1500 bytes are commonplace in a network, you can increase the MTU size to prevent the packets from being fragmented at all. In some cases, you might need to reduce the MTU to avoid having to fragment encrypted packets where the encryption protocols add too much overhead to an already maximum-sized packet. Ideally, the MTU should be increased on every network device and interface along the entire data path.
To adjust the interface MTU from ASDM, first select **Configuration > Device Setup > Interfaces**, select an interface, and click the **Edit** button. Next, select the **Advanced** tab and enter the new MTU value, as shown in Figure 3-21. Although ASDM lets you type a new value, it won't permit the value to change if the interface has not been configured with a name.

To accomplish the same task from the CLI, you can use the following global configuration command to adjust the MTU on an ASA interface:

```
ciscoasa(config)# mtu if_name bytes
```

Identify the interface using its name, such as “inside” or “outside,” rather than the hardware name. The transmitted MTU can be sized from 64 to 9216 bytes.
You should also use the following interface configuration command to enable jumbo frame processing as frames are received on an interface:

```
ciscoasa(config-if)# jumbo-frame reservation
```

Although you can increase the MTU size on any ASA platform, be aware that the `jumbo-frame reservation` command is supported only on the ASA 5585-X.

You can display the current MTU configuration for all firewall interfaces by using the `show running-config mtu` command. Interface MTU settings are also displayed as a part of the `show interface` command output. Example 3-13 shows the output from each of the commands.

**Example 3-13**  *Displaying the Interface MTU*

```
ciscoasa# show running-config mtu
mtu outside 1500
mtu inside 1500

ciscoasa# show interface outside
Interface Ethernet0/0 "outside", is up, line protocol is up
  Hardware is 182546GB rev03, BW 1000 Mbps, DLY 10 usec
  Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
  Input flow control is unsupported, output flow control is unsupported
  MAC address 001a.a22d.1ddc, MTU 1500
```
IP address 192.168.100.10, subnet mask 255.255.255.0
1996 packets input, 127860 bytes, 0 no buffer
Received 533 broadcasts, 0 runts, 0 giants

Verifying Interface Operation

To verify that an ASA interface is operating correctly, you can use the following command:

ciscoasa# show interface if_name

Here, you can specify either a hardware name, such as ethernet0/0, or an interface name, such as outside. The `show interface` command displays the current status, current speed and duplex mode, MAC address, IP address, and many statistics about the data being moved into and out of the interface. The command also lists traffic statistics, such as packets and bytes in the input and output directions, and traffic rates. The rates are shown as 1-minute and 5-minute averages. Example 3-14 shows a sample of the output.

Example 3-14 Sample Output from the `show interface` Command

ciscoasa# show interface ethernet0/0
Interface Ethernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 10 usec
  Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
  Input flow control is unsupported, output flow control is unsupported
  MAC address 001a.a22d.1ddc, MTU 1500
  IP address 192.168.254.2, subnet mask 255.255.255.0
  26722691 packets input, 27145573880 bytes, 0 no buffer
  Received 62291 broadcasts, 0 runts, 0 giants
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  0 pause input, 0 resume input
  0 L2 decode drops
  19039166 packets output, 5820422387 bytes, 0 underruns
  0 output errors, 0 collisions, 0 interface resets
  0 late collisions, 0 deferred
  0 input reset drops, 0 output reset drops
  0 rate limit drops
  input queue (blocks free curr/low): hardware (255/253)
  output queue (blocks free curr/low): hardware (255/255)

Traffic Statistics for "outside":
  26722691 packets input, 27145573880 bytes
  19039166 packets output, 5820422387 bytes
  49550 packets dropped
  1 minute input rate 16 pkts/sec,  16110 bytes/sec
  1 minute output rate 17 pkts/sec,  16240 bytes/sec
  1 minute drop rate, 0 pkts/sec
  5 minute input rate 12 pkts/sec,  13867 bytes/sec
You can verify the interface status in the second line of output. If the interface is shown as “up,” the interface has been enabled. If the line protocol is shown as “up,” there is an active link between the ASA interface and some other device.

To display a summary of all ASA interfaces and their IP addresses and current status, you can use the `show interface ip brief` command, as shown in Example 3-15.

**Example 3-15  Sample Output from the show interface ip brief Command**

```
ciscoasa# show interface ip brief
Interface                  IP-Address      OK? Method Status               Protocol
Ethnernet0/0                192.168.254.2   YES manual up                    up
Ethnernet0/1                10.0.0.1        YES manual up                    up
Ethnernet0/2                unassigned      YES unset  administratively down down
Ethnernet0/3                unassigned      YES unset  administratively down down
Internal-Data0/0            unassigned      YES unset  administratively down up
Management0/0               192.168.1.1     YES manual up                    up
GigabitEthernet1/0          unassigned      YES unset  administratively down down
GigabitEthernet1/1          unassigned      YES unset  administratively down down
GigabitEthernet1/2          unassigned      YES unset  administratively down down
GigabitEthernet1/3          unassigned      YES unset  administratively down down
Internal-Data1/0            unassigned      YES unset  up                    up

ciscoasa#
```

You can monitor the redundant interface status with the following command:

```
ciscoasa# show interface redundant number
```

Example 3-16 shows the output for interface redundant 1. Notice that physical interface Ethernet0/0 is currently the active interface, while Ethernet0/1 is not. The output also reveals the date and time of the last switchover.

**Example 3-16  Verifying the Status of a Redundant Interface**

```
ciscoasa# show interface redundant 1
Interface Redundant1 "inside", is up, line protocol is up
Hardware is i82546GB rev03, BW 100 Mbps, DLY 1000 usec
                  Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
MAC address 0016.c789.c8a5, MTU 1500

[output omitted for clarity]
```
Chapter 3: Configuring ASA Interfaces

**Redundancy Information:**

Member Ethernet0/0(Active), Ethernet0/1

Last switchover at 01:32:27 EDT Sep 24 2010

ciscoasa#

---

**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 from inside the chapter, noted with the Key Topics icon in the outer margin of the page. Table 3-3 lists a reference of these key topics and the page numbers on which each is found.

<table>
<thead>
<tr>
<th>Key Topic Element</th>
<th>Description</th>
<th>Page Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paragraph</td>
<td>Discusses physical interface configuration</td>
<td>83</td>
</tr>
<tr>
<td>Paragraph</td>
<td>Explains redundant interfaces</td>
<td>85</td>
</tr>
<tr>
<td>Paragraph</td>
<td>Describes EtherChannel negotiation with LACP</td>
<td>89</td>
</tr>
<tr>
<td>Paragraph</td>
<td>Explains how to configure a trunk link</td>
<td>95</td>
</tr>
<tr>
<td>Paragraph</td>
<td>Explains how to configure VLAN interfaces on an ASA 5505</td>
<td>97</td>
</tr>
<tr>
<td>List</td>
<td>Describes the three necessary interface security parameters</td>
<td>98</td>
</tr>
<tr>
<td>Paragraph</td>
<td>Describes how to display interface status information and statistics</td>
<td>107</td>
</tr>
</tbody>
</table>

**Define Key Terms**

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

- hardware name
- interface name
- security level
- physical interface
- redundant interface
- member interface
- EtherChannel
- LACP
- VLAN interface
- VLAN trunk link
- MTU

**Command Reference to Check Your Memory**

This section includes the most important configuration and EXEC commands covered in this chapter. It might not be necessary to memorize the complete syntax of every command, but you should be able to remember the basic keywords that are needed.
To test your memory of the commands, cover the right side of Table 3-4 with a piece of paper, read the description on the left side, and then see how much of the command you can remember.

The FIREWALL exam focuses on practical, hands-on skills that are used by a networking professional. Therefore, you should be able to identify the commands needed to configure and test an ASA feature.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>List physical interfaces</td>
<td>ciscoasa# show version</td>
</tr>
<tr>
<td>List interfaces that have a name and security level</td>
<td>ciscoasa# show nameif</td>
</tr>
<tr>
<td>List ASA 5505 interfaces and VLAN mapping</td>
<td>ciscoasa# show switch vlan</td>
</tr>
<tr>
<td>Configure the speed, duplex mode, and state of a physical interface</td>
<td>ciscoasa(config)# interface hardware-id</td>
</tr>
<tr>
<td></td>
<td>ciscoasa(config-if)# speed {auto</td>
</tr>
<tr>
<td></td>
<td>ciscoasa(config-if)# duplex {auto</td>
</tr>
<tr>
<td></td>
<td>ciscoasa(config-if)# [no] shutdown</td>
</tr>
<tr>
<td>Map an ASA 5505 physical interface to a VLAN</td>
<td>ciscoasa(config-if)# switchport access vlan vlan-id</td>
</tr>
<tr>
<td>Define a redundant interface and its member interfaces</td>
<td>ciscoasa(config)# interface redundant number</td>
</tr>
<tr>
<td></td>
<td>ciscoasa(config-int)# member-interface</td>
</tr>
<tr>
<td></td>
<td>physical_interface</td>
</tr>
<tr>
<td></td>
<td>ciscoasa(config-if)# [no] shutdown</td>
</tr>
<tr>
<td>Set the LACP system priority</td>
<td>ciscoasa(config)# lACP system-priority-priority</td>
</tr>
<tr>
<td>Configure a physical interface to become a member of an EtherChannel</td>
<td>ciscoasa(config)# interface type mod/num</td>
</tr>
<tr>
<td></td>
<td>ciscoasa(config-if)# channel-protocol lACP</td>
</tr>
<tr>
<td></td>
<td>ciscoasa(config-if)# channel-group number</td>
</tr>
<tr>
<td></td>
<td>mode [on</td>
</tr>
<tr>
<td></td>
<td>ciscoasa(config-if)# lACP port-priority priority</td>
</tr>
<tr>
<td>Define a physical subinterface that is mapped to a VLAN number</td>
<td>ciscoasa(config)# interface hardware_id.subinterface</td>
</tr>
<tr>
<td></td>
<td>ciscoasa(config-subif)# vlan vlan_id</td>
</tr>
<tr>
<td>Configure an ASA 5505 VLAN interface</td>
<td>ciscoasa(config)# interface vlan vlan-id</td>
</tr>
<tr>
<td>Assign an interface name</td>
<td>ciscoasa(config-if)# nameif if_name</td>
</tr>
</tbody>
</table>
### Table 3-4  Commands Related to ASA Interface Configuration and Verification

<table>
<thead>
<tr>
<th>Task</th>
<th>Command Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign an IP address to an interface</td>
<td>ciscoasa(config-if)# ip address ip-address [subnet-mask]</td>
</tr>
<tr>
<td>Configure an interface to request an IP</td>
<td>ciscoasa(config-if)# ip address dhcp [setroute]</td>
</tr>
<tr>
<td>Assign a security level to an interface</td>
<td>ciscoasa(config-if)# security-level level</td>
</tr>
<tr>
<td>Assign a security level to an interface</td>
<td>ciscoasa(config-if)# security-level level</td>
</tr>
<tr>
<td>Allow traffic to pass between interfaces</td>
<td>ciscoasa(config)# same-security-traffic permit inter-interface</td>
</tr>
<tr>
<td>with the same security level, either</td>
<td>ciscoasa(config)# same-security-traffic permit intra-interface</td>
</tr>
<tr>
<td>across two interfaces or across logical</td>
<td></td>
</tr>
<tr>
<td>interfaces within a single physical</td>
<td></td>
</tr>
<tr>
<td>interface, respectively</td>
<td></td>
</tr>
<tr>
<td>Set the interface MTU size</td>
<td>ciscoasa(config)# mtu if_name bytes</td>
</tr>
<tr>
<td>Allow jumbo Ethernet frames on an ASA</td>
<td>ciscoasa(config-if)# jumbo-frame reservation</td>
</tr>
<tr>
<td>5580</td>
<td></td>
</tr>
<tr>
<td>Display interface details</td>
<td>ciscoasa# show interface if_name</td>
</tr>
<tr>
<td>Display the status of a redundant</td>
<td>ciscoasa# show interface redundant number</td>
</tr>
<tr>
<td>interface</td>
<td></td>
</tr>
<tr>
<td>Display interfaces and their IP addresses</td>
<td>ciscoasa# show interface ip brief</td>
</tr>
<tr>
<td>and status</td>
<td></td>
</tr>
<tr>
<td>Display a summary status of an Ether-</td>
<td>ciscoasa# show port-channel summary</td>
</tr>
<tr>
<td>Channel and its member interfaces</td>
<td></td>
</tr>
</tbody>
</table>
Index

Numbers

4GE (4-port Gigabit Ethernet), 24

A

AAA (Authentication, Authorization, and Accounting) services, 587-588
command authorization, configuring, 214-222
management access, controlling and verifying, 201-224
NAT (Network Address Translation), integration, 294
remote accounting, configuring, 222-223
servers, 208
testing, 214
user authentication, configuring, 591-596
abbreviating, commands, 42
access control, 386-391, 397
access rules, organizing using object groups, 438-450
configuring, 454-457
default rules, 410-411
global ACL, 411-412
interface access rules, 405-409
  configuring, 412-427
  verifying, 432-438
NAT (Network Address Translation), integration, 335-336
object groups, verifying, 450-453
state tables, 397-409
time-based access rules, 427-432
troubleshooting, 457-463
user-based proxy, 587
verifying, 454-457
access list lookup (Packet Tracer), 737
active-active failover, 675, 677-678
  configuring, 692-701
active-standby failover, 675-676
  configuring, 683-691
Adaptive Security Appliances (ASA).
  See ASA (Adaptive Security Appliances)
Adaptive Security Device Manager (ASDM).
  See ASDM (Adaptive Security Device Manager)
Add Access Rule dialog box, 413
Add Network Object dialog box, 440
Add Network Object Group dialog box, 441
Add TCP Service Group dialog box, 444
address translation, 275-280
addresses. see also NAT (Network Address Translation)
  address deployment, 291-292
  auto, 361-363
comparing configurations, 360-361
configuring auto, 343-349
configuring dynamic identity, 325-326
configuring network static inside, 315-317
configuring outside, 330-333
configuring static identity, 326-328
configuring static inside, 312-315
configuring static inside policy, 320-323
control, 340
deployment, 291-292, 295-296
DNS Rewrite, 333-335
enforcing, 290-291
input parameters, 292-293
integrating with access control, 335-336
integrating with MPF, 336
limitations, 380
manual, 363-369
network objects, 339
PAT (Port Address Translation), 292-293
rule priority, 330, 340
troubleshooting, 382
tuning, 380-381

verifying dynamic inside, 311-312
verifying static inside, 323-324
PAT (Port Address Translation), configuring dynamic inside, 304-308
admin context, 659
changing, 662
administration, failover, 705
Advanced Inspection and Prevention Security Services Module (AIP-SSM), See AIP-SSM
AIC (application inspection and control) filtering
firewalls, 15
stateful packet filtering, 12-13
AIP (Advanced Inspection and Prevention), SSMs (Security Services Modules), 22-23
AIP-SSM (Advanced Inspection and Prevention Security Services Module), 715, 720
configuring, 723-724
failure management mode, 722
initializing, 723
inline operation, 720
installing, 721-724
ALG (application layer gateway), firewalls, 14-15
application inspection and control (AIC). See AIC (application inspection and control)
ARP (Address Resolution Protocol), transparent firewall mode, 642-645
ASA (Adaptive Security Appliances), 2
  configuration files, 54-58
  factory default configuration, 52-54
  licenses, selecting, 29-31
  reloading, 34, 63-70
ASA 5585-X, 24-25
  memory requirements, 31-32
  SSMs (Security Services Modules), 22-25
  traffic performance, 25-29
ASA File System, 48-63
ASA models
  ASA 5550, 20-21
  ASA 5580, 21-22
ASDM (Adaptive Security Device Manager), 34, 47-52
  Configuration view, 51
  event viewer, 264-265
  file system management, 171-172
  Home view, 50
  images, managing, 177-178
  interface access rules, managing, 434-437
  interfaces, viewing list of, 80
  Monitoring view, 52
  Packet Capture, 742-746
  saving installer file, 49
  security policies, creating, 490-495
ASDM Public Server Wizard, 424-425
asymmetric routing, detecting, 703-705
authentication
  AAA (Authentication, Authorization, and Accounting), management access, 201-224
  configuring, 166-168, 598-600
  direct HTTP, 589-590
direct Telnet, 590-591
password-only, 205
prompts, configuring, 596-597
timeouts, configuring, 598
user-based proxy, 586-587
verifying, 595
Authentication, Authorization, and Accounting (AAA). See AAA (Authentication, Authorization, and Accounting)
auto NAT
  configuring, 343-349
dynamic translations, configuring, 352-357
static port translations, configuring, 349-351
translations, configuring, 373-375
verifying, 361-363

B
bandwidth, traffic, controlling, 616-624
base license (ASA), 30
BEQ (best-effort queue), 612
Botnet Traffic Filter, 15
botnet traffic, filtering, 15, 561-570
bridge groups, transparent firewall mode, 634
Browse Service dialog box, 413, 446-447
Browse Source dialog box, 413
buffer contents, copying capture, 751-752

C
capture type asp-drop command, 758-759
capturing packets, 752-759
category-based URL filtering, firewalls, 16
CCNP Security 642-618 FIREWALL exam, updates, 777
cd command, 174
CERT practice test engine, 765-769
Cisco ASA licenses, selecting, 29-31
Cisco ASA models
  ASA 5550, 20-21
  ASA 5580, 21-22
  ASA 5585-X, 24-25
  memory requirements, 31-32
  selecting, 18-29
  SSMs (Security Services Modules), 22-25
  traffic performance, 25-29
Cisco Learning Network, 767
class maps, Layer 3-4, defining, 484-486
classes, resource, creating, 663-665
CLI (command line interface), 34, 40-52
  command output, searching and filtering, 45-47
  commands
    entering, 41-43
    history, 45
  context-based help, 43-45
  file system management, 172-176
  global configuration mode, 41
  interface access rules, managing, 437-438
  interrupted command lines, redisplaying, 43
  packets, capturing, 746-751
  privileged EXEC mode, 40
  ROMMON mode, 41
  terminal screen format, 47
  user EXEC mode, 40
code listings
  Abbreviating an ASA Command, 42
  Adding Packet Tracer Information to a Packet Capture, 760-761
  Applying a Policy Map as a Service Policy, 490
  Applying an HTTP Inspection Policy Map, 527
  ASA Bootup Sequence, 68
  ASA Pointing Out a Syntax Error, 44
  ASA VLAN CLI Configuration, 98
  Assigning an Interface Name, 99
  Attempting to Create a Duplicate Directory Name, 174
  Better Approach to Permitting Access for a Dynamic Protocol, 515
  capture Command Limited to ACL Drops, 460
  Capturing Dropped Packets Due to an Interface ACL, 759
  Capturing Dropped Packets Due to Unexpected TCP SYN, 759
  Changing Directory and Confirming Location, 175
  clear conn Command Usage, 402
  Clearing Portions of an ASA Running Configuration, 58
  Commands to Configure the Access Lists, 640
  Commands Used to Configure a Capture Session, 748
  Commands Used to Configure Static Routes, 638
  Commands Used to Configure the TCP Normalizer, 503
  Configuration Commands, 150
  Configuration Commands Used for EIGRP Scenario, 142
  Configuring a Management Class Map and Policy Map, 560
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring a Policy Map with Three Security Policies</td>
<td>489</td>
</tr>
<tr>
<td>Configuring a Redundant Interface Pair</td>
<td>87</td>
</tr>
<tr>
<td>Configuring a Regular Expression to Match “/customer”</td>
<td>525</td>
</tr>
<tr>
<td>Configuring a Resource Class</td>
<td>665</td>
</tr>
<tr>
<td>Configuring a Traffic Policer to Control Outbound HTTP Traffic</td>
<td>620</td>
</tr>
<tr>
<td>Configuring a Trunk Link on an ASA</td>
<td>96</td>
</tr>
<tr>
<td>Configuring an EtherChannel Using the CLI</td>
<td>94</td>
</tr>
<tr>
<td>Configuring an EtherType Access List for Non-IP Traffic</td>
<td>641</td>
</tr>
<tr>
<td>Configuring ARP Inspection</td>
<td>645-646</td>
</tr>
<tr>
<td>Configuring Botnet Traffic Filtering</td>
<td>570</td>
</tr>
<tr>
<td>Configuring Failover on the Primary ASA</td>
<td>691-699</td>
</tr>
<tr>
<td>Configuring Failover on the Secondary ASA</td>
<td>691-701</td>
</tr>
<tr>
<td>Configuring Global HTTP Inspection</td>
<td>511</td>
</tr>
<tr>
<td>Configuring HTTP Inspection for Specific Traffic on an Interface</td>
<td>511</td>
</tr>
<tr>
<td>Configuring HTTP Inspection on a Nonstandard Port</td>
<td>512</td>
</tr>
<tr>
<td>Configuring Interfaces in Transparent Firewall Mode</td>
<td>636</td>
</tr>
<tr>
<td>Configuring Regular Expressions to Match “http://” or “https://”</td>
<td>525</td>
</tr>
<tr>
<td>Configuring the ASA Interface</td>
<td>103</td>
</tr>
<tr>
<td>Configuring the ContextA Outside Interface for ASR Group 1</td>
<td>705</td>
</tr>
<tr>
<td>Configuring the ContextB Outside Interface for ASR Group 1</td>
<td>705</td>
</tr>
<tr>
<td>Configuring the DHCP Relay Agent Feature</td>
<td>119</td>
</tr>
<tr>
<td>Configuring the DHCP Server Feature</td>
<td>122</td>
</tr>
<tr>
<td>Configuring the Management Interface for the AIP-SSC</td>
<td>722</td>
</tr>
<tr>
<td>Configuring the Primary ASA “admin” Context Interfaces for Failover</td>
<td>700</td>
</tr>
<tr>
<td>Configuring the Primary ASA “ContextA” Interfaces for Failover</td>
<td>700</td>
</tr>
<tr>
<td>Configuring the Primary ASA “ContextB” Interfaces for Failover</td>
<td>700</td>
</tr>
<tr>
<td>Configuring Three Class Maps</td>
<td>486</td>
</tr>
<tr>
<td>Configuring Traffic Shaping</td>
<td>623</td>
</tr>
<tr>
<td>Configuring User Authentication at the CLI</td>
<td>594</td>
</tr>
<tr>
<td>Copying Files to an ASA File System</td>
<td>61</td>
</tr>
<tr>
<td>Creating a Default RSA Key Pair</td>
<td>192</td>
</tr>
<tr>
<td>Default DNS Inspection Policy Map Configuration</td>
<td>548</td>
</tr>
<tr>
<td>Default Interface Configuration on ASA 5510 and Higher Models</td>
<td>82</td>
</tr>
<tr>
<td>Default Interface Configuration on the ASA 5505</td>
<td>82</td>
</tr>
<tr>
<td>Deleting a File in an ASA File System</td>
<td>63</td>
</tr>
<tr>
<td>Determining ASA Hardware Platform, OS Image, and Release Information</td>
<td>64</td>
</tr>
<tr>
<td>Disabling MAC Address Learning</td>
<td>647</td>
</tr>
<tr>
<td>Displaying a Class Map Configuration</td>
<td>481</td>
</tr>
<tr>
<td>Displaying a Policy Map Configuration</td>
<td>480</td>
</tr>
<tr>
<td>Displaying Capture Sessions</td>
<td>748</td>
</tr>
<tr>
<td>Displaying Device Identity</td>
<td>168</td>
</tr>
<tr>
<td>Displaying Information About Static Route Tracking</td>
<td>131</td>
</tr>
<tr>
<td>Displaying Information About Traffic Policing</td>
<td>621</td>
</tr>
<tr>
<td>Displaying Information About Traffic Shaping</td>
<td>624</td>
</tr>
</tbody>
</table>
Displaying Object Definitions, 362
Displaying the Activity of the Default Dynamic Protocol Inspectors, 508
Displaying the ASA 5505 Interface-to-VLAN Mapping, 83
Displaying the Contents of a Packet Capture Session, 749
Displaying the Current Interface Queue Sizes, 615
Displaying the Default Dynamic Protocol Inspector Configuration, 509
Displaying the Default Service Policies, 480
Displaying the Interface MTU, 106
Displaying the Routing Table Contents with show route, 152
Displaying the Startup Configuration Contents, 54
Displaying Virtual Reassembly Activity, 612
Enabling Basic Threat Detection, 576
Enabling DNS Parameter Inspection, 547
Enabling ICMP and ICMP Error Inspection Globally, 506
Help Output Generated from the help passwd Command, 44
Inserting ACEs into an Existing ACL, 438
Listing Physical ASA Interfaces, 81
Listing the Contents of an ASA Flash File System, 59
Log Messages for TCP Session Setup and Teardown, 405
Manually Downloading an Image File in ROMMON Mode, 70
Manually Reloading an ASA, 66
Mapping Interfaces to VLANs on an ASA 5505, 84
MPF Structure for Protocol Inspection, 507
MPF Structure for Sending Matched Packets into an LLQ, 616
MPF Structure for the TCP Normalizer, 502
MPF Structure for Traffic Policing, 620
MPF Structure for Traffic Shaping, 622
NAT Table Displayed, 342
packet-tracer Command Usage, 461
Performing a File System Check and Deleting .REN Files, 175
Performing Password Recovery, 233
Preparing to Boot a Different Operating System Image File, 65
Redisplaying an Interrupted Command Line, 43
Remotely Executing the show version Command on a Failover Peer, 705
Removing a Directory from the Local File System, 174
Renaming a File, 173
Renaming a File in an ASA File System, 62
Returning an ASA to the Factory Default Configuration, 53
RIPv2 Example Configuration, 135
Sample Dynamic Configuration from OS Version 8.2, 360
Sample Dynamic Configuration from OS Version 8.3, 361
Sample Hybrid NAT Configuration from OS Version 8.2, 379
Sample Hybrid NAT Configuration from OS Version 8.3, 379
Sample Output from the show failover history Command, 708
Sample Output from the show interface Command, 107
Sample Output from the show interface ip brief Command, 108
Verifying the Botnet Traffic Filter License Status, 564
Verifying the Current Firewall Mode, 635
Verifying the Status of a Redundant Interface, 108
Verifying User Authorization Information, 600
Viewing AAA Server Statistics, 224

command lines, interrupted, redisplaying, 43
command output, searching and filtering, 45-47
command-line interface (CLI). See CLI (command line interface)
commands
abbreviating, 42
authorization, AAA (Authentication, Authorization, and Accounting), 214-222
capture type asp-drop, 758-759
cd, 174
CLI (command line interface), entering, 41-43
copy, 173
delete, 173
dir, 172
disk, 172
fsck, 175
history, 45
mapping, 149-150
mkdir, 174
more, 173
ping, 733-734
ping tcp, 735
pwd, 175
rename, 173
rmdir, 174
show access-list, 433-452
show access-list brief, 434
show clock, 251-432
show conn, 400
show conn detail, 400
show context, 661
show failover, 706-708
show interface, 107
show interface ip brief, 108
show local-host, 404
show nat detail, 382
show port-channel summary, 94
show route, 152
show running-config access-list, 451
show shun, 456
show version, 705
shun, 456
traceroute, 736
configuration
access control, 454-457
active-active failover, 692-701
AIP-SSM (Advanced Inspection and Prevention Security Services Module), 723-724
authorization, 166-168
prompts, 596-597
timeouts, 598
CSC-SSM (Content Security and Control Security Service Module), 725
default, 34
DHCP relay, 117-119
DHCP server, 119-122
direct Telnet, 596
DNS server groups, 168-171
EtherChannels, 87-95
event destinations, 262
event filters, 261-262
event logging, 255-271
factory default, 52-54
failover
  *active-standby, 683-691*
  *health monitoring, 702-703*
  *timers, 701-702*
global ACL, 421-424
global logging properties, 256-258
HTTP inspection, 507-513, 518-520
interface access rules, 412-427
interfaces, MTUs (maximum transmission units), 104-107
management access, 186-224
  *remote, 188-189*
manual NAT, 363-369
monitoring, SNMP, 225-229
MPF (Modular Policy Framework), 482-483
NAT (Network Address Translation)
  *auto, 343-349*
  *bypass, 328-330*
  *control, 296-298*
  *dynamic identity, 325-326*
  *dynamic inside NAT, 298-304*
  *static inside, 312-315*
  *static inside policy, 320-323*
  *twice, 370-373*
no-translation rules, 324-325
out-of-band management interface, 189
PAT (Port Address Translation),
  *dynamic inside, 304-308*
physical interfaces, 80-95
regular expressions, 525-526
resource management, 663-665
Security Contexts, 658-661
session logging, 255-271
static routing, 124-132
system time, 247-252
traffic policers, 618-621
transparent firewall mode, 635-639
trunk lists, 96
unidirectional manual static NAT, 376-377
user authentication, 591-600
user session accounting, 601-602
user-based proxy, 588-591
virtual firewalls, 658
VLAN interfaces, 95-98
configuration files, 34, 54-58
Configuration view (ASDM), 51
connection limits, Layer 3-4, tuning, 495-499
connection tables, 398-401
connections
  *inbound/outbound, 403*
  *inside/outside, 403*
context-based help, CLI (command line interface), 43-45
controlling traffic, transparent firewall mode, 639-642
copy command, 173
copying, files to file system, 61
cryptographic Unified Communications (UC) proxy, firewalls, 16
CSC (Content Security and Control), SSMs (Security Services Modules), 23
CSC-SSM (Content Security and Control Security Service Module), 719-720
configuring, 725
Ethernet connections, 724
initialization, 725
installing, 724
integration, 724-725
cut-through proxy, 586-589
troubleshooting, 602-603
DDNS, firewalls, 17
default access rules, 410-411
defining
  Layer 3-4 class maps, 484-486
  Layer 3-4 policy maps, 486-490
delete command, 173
deleting, files, 63
deployment
  DHCP services, 117-122
  SSMs (Security Service Modules), 719
  virtual firewalls, 656-658
destinations, log messages, 252-253
devices
  identities, configuring, 165-166
  images, verifying, 185-186
  settings, 165-168
DHCP, firewalls, 17
DHCP services, deploying, 117-122
dir command, 172
direct HTTP authentication, 589-590
direct Telnet, configuring, 596
direct Telnet authentication, 590-591
directories, removing, 174
directory names, duplicate, creating, 174
displaying
  static routes, 152
  virtual reassembly activity, 612
DNS Rewrite, NAT (Network Address Translation), 333-335
DNS server groups, configuring, 168-171
domains, security, firewalls, 8-10
DoS (Denial of Service) prevention, firewalls, 16
downloadable ACLs, configuring, 600
dropped packets, capturing, 752-759
duplicate directory names, creating, 174
dynamic identity NAT, configuring, 325-326
dynamic inside NAT
  configuring, 298-304
  verifying, 311-312
dynamic inside policy NAT, configuring, 308-311
dynamic NAT, 295
  comparing configurations, 360-361
dynamic PAT, 295
dynamic protocols, inspecting, 507-516

E
Edit Access Rule dialog box, 8.495
editing, Security Contexts, 663
egress interfaces, selecting, 384
EIGRP (Enhanced Interior Gateway Routing Protocol), routing with, 135-142
email, log messages, 267-269
enforcing, NAT (Network Address Translation), 290-291
Enhanced Interior Gateway Routing Protocol (EIGRP), routing with, 135-142
ESP (IPsec), 398
EtherChannels, 16
  configuring, 87-95
  negotiation methods, 89
Ethernet connections, CSC-SSM (Content Security and Control Security Service Module), 724
event destinations, configuring, 262
event filters, configuring, 261-262
event logging
configuring, 255-271
implementing, 272-273
managing, 252-255
troubleshooting, 273-274
verifying, 271-273
event viewer, ASDM (Adaptive Security Device Manager), 264-265
events
Abbreviating an ASA Command, 42
Adding Packet Tracer Information to a Packet Capture, 760-761
Applying a Policy Map as a Service Policy, 490
Applying an HTTP Inspection Policy Map, 527
ASA Bootup Sequence, 68
ASA Pointing Out a Syntax Error, 44
ASA VLAN CLI Configuration, 98
Assigning an Interface Name, 99
Attempting to Create a Duplicate Directory Name, 174
Better Approach to Permitting Access for a Dynamic Protocol, 515
capture Command Limited to ACL Drops, 460
Capturing Dropped Packets Due to an Interface ACL, 759
Capturing Dropped Packets Due to Unexpected TCP SYN, 759
Changing Directory and Confirming Location, 175
clear conn Command Usage, 402
Clearing Portions of an ASA Running Configuration, 58
Commands to Configure the Access Lists, 640
Commands Used to Configure a Capture Session, 748
Commands Used to Configure Static Routes, 638
Commands Used to Configure the TCP Normalizer, 503
Configuration Commands, 150
Configuration Commands Used for EIGRP Scenario, 142
Configuring a Management Class Map and Policy Map, 560
Configuring a Policy Map with Three Security Policies, 489
Configuring a Redundant Interface Pair, 87
Configuring a Regular Expression to Match “/customer”, 525
Configuring a Resource Class, 665
Configuring a Traffic Policer to Control Outbound HTTP Traffic, 620
Configuring a Trunk Link on an ASA, 96
Configuring an EtherChannel Using the CLI, 94
Configuring an EtherType Access List for Non-IP Traffic, 641
Configuring ARP Inspection, 645-646
Configuring Botnet Traffic Filtering, 570
Configuring Failover on the Primary ASA, 691-699
Configuring Failover on the Secondary ASA, 691-701
Configuring Global HTTP Inspection, 511
Configuring HTTP Inspection for Specific Traffic on an Interface, 511
Configuring HTTP Inspection on a Nonstandard Port, 512
Configuring Interfaces in Transparent Firewall Mode, 636
Configuring Regular Expressions to Match “http://” or “https://”, 525
Listing the Contents of an ASA Flash File System, 59
Log Messages for TCP Session Setup and Teardown, 405
Manually Downloading an Image File in ROMMON Mode, 70
Manually Reloading an ASA, 66
Mapping Interfaces to VLANs on an ASA 5505, 84
MPF Structure for Protocol Inspection, 507
MPF Structure for Sending Matched Packets into an LLQ, 616
MPF Structure for the TCP Normalizer, 502
MPF Structure for Traffic Policing, 620
MPF Structure for Traffic Shaping, 622
NAT Table Displayed, 342
pack-tracer Command Usage, 461
Performing a File System Check and Deleting .REN Files, 175
Performing Password Recovery, 233
Preparing to Boot a Different Operating System Image File, 65
Redisplaying an Interrupted Command Line, 43
Remotely Executing the show version Command on a Failover Peer, 705
Removing a Directory from the Local File System, 174
Renaming a File, 173
Renaming a File in an ASA File System, 62
Returning an ASA to the Factory Default Configuration, 53
RIPv2 Example Configuration, 135
Sample Dynamic Configuration from OS Version 8.2, 360
Sample Hybrid NAT Configuration from OS Version 8.2, 379
Sample Hybrid NAT Configuration from OS Version 8.3, 379
Sample Output from the show failover history Command, 708
Sample Output from the show interface Command, 107
Sample Output from the show interface ip brief Command, 108
Sample Output of the show failover Command in Active-Active Mode, 707
Sample Output of the show failover Command in Active-Standby Mode, 706
Sample Static Configuration from OS Version 8.2, 352
Sample Static Configuration from OS Version 8.3, 352
Searching through Command Output, 46
Secure Approach to Permitting Access for a Dynamic Protocol, 516
show access-list brief Command Output, 434
show access-list Command Output, 433
show access-list Output with Object Groups, 452
show clock Command Usage, 432
show conn Command Output, 400
show conn detail Command Output, 400
show context Command Output, 661
show local-host Command Output, 404
show nat Command Output with Auto NAT Only, 362
show nat detail Command Output, 382
show port-channel summary Command Output, 94
show running-config access-list Output with Object Groups, 451
show running-config nat Command Output, 361
show shun Command Usage, 456
show xlate Command Output, 363
show xlate Command Output (NAT), 311
show xlate Command Output (PAT), 311
show xlate detail Command Output, 312-324
shun Command Usage, 456
Simple Hierarchy of the Default MPF Configuration, 481
Static Route Tracking Configuration, 131
Testing a Regular Expression Before Configuration, 526
Testing AAA Authentication, 214
Using a New Startup Configuration File, 56
Using a Single Regexp to Match “http://” or “https://”, 526
Using Conext-Based Help, 43
Using Context-Based Help to List Possible Commands, 44
Using Packet Tracer to Test ASA Rules for an Inbound HTTP Packet, 741
Using Packet Tracer to Test ASA Rules for an Inbound HTTPS Packet, 740-741
Using the ping Command Alone to Prompt for Arguments, 734
Using the ping Command to Test Reachability, 733
Using the ping tcp Command to Test TCP Reachability, 735
Using the traceroute Command to Discover a Network Path, 736
Verifying ARP Inspection Status, 645
Verifying Basic Authentication, 168
Verifying Device Image and License Information, 185-186
Verifying DNS Resolution, 170
Verifying Logging, 271
Verifying Logging Queue Performance, 274
Verifying NetFlow Export, 272
Verifying System Time with show clock, 251
Verifying System Time with show ntp associations, 252
Verifying the Botnet Traffic Filter License Status, 564
Verifying the Current Firewall Mode, 635
Verifying the Status of a Redundant Interface, 108
Verifying User Authorization Information, 600
Viewing AAA Server Statistics, 224
expression operators, 46

F

factory default configuration, 34, 52-54
failover, 675
  active-active, 675-678
    configuring, 692-701
  active-standby, 675-676
    configuring, 683-691
administering, 705
asymmetric routing, detecting, 703-705
health monitoring, configuring, 702-703
leverage, 708-709
operation
  tuning, 701-706
  verifying, 706-708
roles, 675-681
timers, configuring, 701-702
ASDM (Adaptive Security Device Manager), 171-172
CLI (command line interface), 172-176
failover clustering, firewalls, 16
failure, ASAs, detecting, 681-683
failure management mode, AIP-SSM (Advanced Inspection and Prevention Security Services Module), 722
feature licenses (ASA), 30
File System, 34, 48-63
management, 171-176
files
- copying to ASA file system, 61
- deleting, 63
- displaying contents, 60
- File System, 60
- renaming, 62-173
- upgrading, local computers, 179-181
filtering
- botnet traffic, 561-570
- command output, 45-47
- stateful, 406-408
firewall mode, 632-639
- bridge groups, 634
- routed, 632-635
- transparent, 626-628, 633-635
  - ARP (Address Resolution Protocol), 642-645
  - configuring, 635-639
  - controlling traffic in, 639-642
  - disabling MAC address learning, 645-647
firewalls, 7-10, 649-650
  - AIC (application inspection and control)
    - filtering, 15
  - ALG (application layer gateway), 14-15
  - category-based URL filtering, 16
  - Cisco ASA models, selecting, 18-29
  - cryptographic Unified Communications (UC) proxy, 16
  - DDNS, 17
  - DHCP, 17
  - DoS (Denial of Service) prevention, 16
  - EtherChannels, 16
  - features, 15-18
  - IDS (intrusion detection system), 7
  - IP multicasting, 17
  - IP routing functionality, 17
  - IPS (intrusion prevention system), 7-10
  - IPv6, 17
  - NAT (Network Address Translation), 17
  - NBA (network behavior analysis), 14
  - NIPS (network intrusion prevention system), 13
  - policy virtualization, 17
  - PPPoE clients, 17
  - redundant interfaces, 16
  - remote access VPNs, 16
  - Reputation-based Botnet Traffic Filtering, 15
  - security domains, 8-10
  - session auditing, 15
  - site-to-site VPNs, 16
  - SSMs (Security Services Modules), 15
  - stateful packet filtering, 12-13
  - stateless packet filtering, 11-12
  - techniques, 11-15
  - traffic correlation, 16
  - traffic virtualization, 17
  - user-based access control, 15
  - virtual
    - configuring, 658-661
    - creating, 650-651, 654-656
    - deployment, 656-658
    - managing, 661-663
    - resource management, 663-665
    - Security Contexts, 654-655
    - troubleshooting, 665-666
    - verifying, 661
flags, TCP connection, 401-402
flash file system, 59-60
flow creation (Packet Tracer), 737
flow lookup (Packet Tracer), 737
formats, messages, logging, 254
fragmented traffic, handling, 610-611
fsck command, 175

G-H

global ACL, 411-412
    configuring, 421-424
global configuration mode (CLI), 41
global logging properties, configuring, 256

handling traffic
    controlling bandwidth, 616-624
    fragmented, 610-611
    prioritization, 612-616
health monitoring, configuring, 702-703
help, context-based, 43-45
high availability failover clustering, firewalls, 16
history, commands, 45
Home view (ASDM), 50
HTTP (HyperText Transfer Protocol)
    redirection, 590
        configuring, 595
    virtual, 590
HTTP inspection
    configuring, 507-513, 518-520
    policy maps, applying, 526
HTTPS (HTTP Secure), remote management access, configuring, 194

I-K

ICMP
    connections, 398
        traffic inspection, configuring, 503-506
identities, devices, configuring, 165-166
identity certificates, deploying, 197-199
IDS (intrusion detection system) versus IPS (intrusion prevention system), 7
images, ASDM (Adaptive Security Device Manager), managing, 177-178
improper translation, NAT (Network Address Translation), 382-384
initialization
    AIP-SSM (Advanced Inspection and Prevention Security Services Module), 723
    CSC-SSM (Content Security and Control Security Service Module), 725
inline operation, SSMs (Security Services Modules), 720
input parameters, NAT (Network Address Translation), 293-295
inspecting traffic, 465-473
    botnet, 561-570
    dynamic protocol, 507-516
    MPF (Modular Policy Framework), 479-483
        configuring, 482-483
    OSI Layers 3-4, 484-506
    OSI Layers 5-7, 517-561
    threat detection, 570-578
installation
    AIP-SSM (Advanced Inspection and Prevention Security Services Module), 721-724
    CSC-SSM (Content Security and Control Security Service Module), 724
installer file (ASDM), saving, 49
interface access rules, verifying, 432-438
interfaces
  access rules, 405-409
    configuring, 412-427
    logging, 417-421
egress, selecting, 384
MTUs (maximum transmission units), configuring, 104-107
names, assigning, 99
operations, verifying, 107-109
physical
  configuring, 80-95
  listing, 80-82
policy maps, applying to, 490
redundant, 16, 84-87
security levels, 408
  setting, 100-104
security parameters, configuring, 98-104
VLANs (virtual LANs), configuring, 95-98
internal buffers, logging to, 262-264
IP addresses, interfaces, assigning, 99-100
IP multicasting, firewalls, 17
IP options lookup (Packet Tracer), 737
IP routing, firewalls, 17
IP telephony, proxy services, 603
IPS (intrusion prevention system) versus IDS (intrusion detection system), 7
IPv6, firewalls, 17

Layer 3-4
  class maps, defining, 484-486
  connection limits, tuning, 495-499
  inspecting, 484-506
  policy maps, defining, 486-490
Layer 5-7, inspecting, 517-561
leveraging, failover, 708-709
licenses
  ASA, selecting, 29-31
  managing, 182-183
  verifying information, 185-186
listing physical interfaces, 80-82
LLQ (low-latency queue), 613
local computers, upgrading files from, 179-181
local databases, creating users in, 203-205
local file system, directories, removing, 174
local host tables, 403-404
log messages
  email, 267-269
  sending, destinations, 252-253
logging
  event
    configuring, 255-271
    implementation, 272-273
    managing, 252-255
    troubleshooting, 273-274
    verifying, 271-273
  messages, formats, 254
session
  configuring, 255-271
  implementation, 272-273
  managing, 252-255
  troubleshooting, 273-274
  verifying, 271-273
state tables, 405
low-latency queue (LLQ), 613
MAC addresses, disabling learning, 645-647
management access
  configuring, 186-224
  controlling with AAA, 201-224
remote
  configuring, 188-189
  troubleshooting, 230-231
management access banners, 199-201
  configuring, 199-201
Management Information Bases (MIB), 225
managing
  event logging, 252-255
  file system, 171-176
  session logging, 252-255
  software, 176-186
man-in-the-middle attacks, spoofed ARP attacks, 643
manual NAT
  configurations, comparing, 378-380
  configuring, 363-369
  rules, inserting, 377
  translations, configuring, 373-375
manually configuring, active-standby failover, 683-691
map commands, 149-150
mapping, ASA 5505 interfaces to VLANs, 84
MARS (Monitoring, Analysis, and Response System), 719
memory requirements, 31-32
messages
  altering settings, 258-261
  formats, logging, 254
  severity levels, 255
metacharacters, regular expressions, 524-525
mkdir command, 174
mobility proxy, 603
Modular Policy Framework (MPF). See MPF (Modular Policy Framework)
module components, SSMs (Security Service Modules), 718-719
monitoring, configuring, SNMP, 225-229
Monitoring, Analysis, and Response System (MARS), 719
Monitoring view (ASDM), 52
more command, 173
MPF (Modular Policy Framework), 479-482
  configuring, 482-483
NAT (Network Address Translation), integration, 336
  protocol inspection, 507
  TCP normalizer, 502
MTUs (maximum transmission units), interfaces, configuring, 104-107
names, interfaces, assigning, 99
NAT (Network Address Translation), 288-290, 737
AAA (Authentication, Authorization, and Accounting), integration, 294
  access control, integrating, 335-336
  address deployment, 291-292
auto
  configuring, 343-349, 352-357
  verifying, 361-363
bypass, configuring, 328-330
  control, 295-340
  configuring, 296-298
deployment, 295-296
DNS Rewrite, 333-335
dynamic, 295
  comparing configurations, 360-361
dynamic identity, configuring, 325-326
dynamic inside
  configuring, 298-304
  verifying, 311-312
dynamic inside policy, configuring, 308-311
enforcing, 290-291
exemption, 295, 296
firewalls, 17
implementing in early versions of ASA, 290-339
implementing in later versions of ASA, 339-384
improper translation, 337, 382-384
incompatible protocols, 337
input parameters, 293-295
limitations, 380
manual, configuring, 363-369
MPF (Modular Policy Framework), integration, 336
network objects, 339
network static inside, configuring, 315-317
no-translation rules, configuring, 324-325
outside, configuring, 330-333
versus PAT (Port Address Translation), 292-293
policy, 295
proxy ARP, 338
rule priority, 330, 340
static, 295
  comparing configurations, 351-352
static identity, configuring, 326-328
static inside
  configuring, 312-315
  verifying, 323-324
static inside policy, configuring, 320-323
syslog messages, 338
tables, 341-343
translations, 373-375
troubleshooting, 382
tuning, 380-381
twice, configuring, 370-373
NAT rules
  inserting manual, 377
  object groups, 357-360
  unidirectional manual static NAT, configuring, 376-377
NBA (network behavior analysis), firewalls, 14
negotiation methods, EtherChannels, 89
NetFlow, support, 254
Network Address Translation (NAT). See NAT (Network Address Translation)
network behavior analysis (NBA). See NBA (network behavior analysis)
network connectivity, testing, 733-736
network intrusion prevention system (NIPS). See NIPS (network intrusion prevention system)
network objects, NAT (Network Address Translation), 339
network static inside NAT, configuring, 315-317
NIPS (network intrusion prevention system), firewalls, 13
no-translation rules, configuring, 324-325
NTP, system time, 249-252
object groups
access rules, verifying, 438-450
NAT rules, 357-360
verifying, 450-453
operations, interfaces, verifying, 107-109
OS version 8.3, upgrading to, 181
OSI Layers 3 and 4, inspecting, 484-506
OSI Layers 5-7, inspecting, 517-561
OSPF (Open Shortest Path First), routing with, 142-153
out-of-band management interface, configuring, 189

Packet Capture, 459-460, 742-761
ASDM (Adaptive Security Device Manager), 742-746
buffer contents, copying capture, 751-752
CLI (command line interface), capturing packets, 746-751
dropped packets, capturing, 752-759
Packet Tracker, combining, 760-761
packet filtering
stateful, 12-13
stateless, 11-12
packet shunning, 455-457
Packet Tracer, 460-462, 737-742
   Packet Capture, combining, 760-761
packets, classification, 655-656
parameters, physical interfaces, configuring, 83-84
password-only authentication, 205
passwords, recovery, 232-234

PAT (Port Address Translation)
dynamic, 295
dynamic inside
   configuring, 304-308
   verifying, 311-312
incompatible protocols, 337
versus NAT (Network Address Translation), 292-293
static, 295
static inside
   configuring, 317-320
   verifying, 323-324
permanent self-signed certificates, creating, 194
per-user cryptographic UC proxy licenses (ASA), 31
per-user override, 599-600
per-user premium SSL VPN licenses (ASA), 31
phone proxy, 603
physical interfaces
   configuring, 80-95
   listing, 80-82
ping command, 733-734
ping tcp command, 735
PKI (Public Key Infrastructure)
   encryption, identity certificates, obtaining, 194
platform-specific license (ASA), 30
policies
   OSI Layers 3 and 4, inspecting, 484-506
   security, ASDM (Adaptive Security Device Manager), 490-495
   virtualization, 17
policing, traffic, 617-621
policy maps
   HTTP inspection, 526
   interfaces, applying to, 490
   Layer 3-4, defining, 486-490
policy NAT, 295
PPPoE clients, 17
presence federation proxy, 603
prioritizing, traffic, 612-616
privileged EXEC mode (CLI), 40
promiscuous operation, SSMs (Security Services Modules), 721
prompts, authentication, configuring, 596-597
protocols
dynamic, inspecting, 507-516
NAT (Network Address Translation), incompatible, 337
PAT (Port Address Translation), incompatible, 337
statefully tracked information, 398
proxy ARP, NAT (Network Address Translation), 338
proxy services
IP telephony, 603
phone proxy, 603
presence federation proxy, 603
TLS proxy, 603
unified telepresence, 603
user-based proxy, 586-589
configuring, 588-589, 591
troubleshooting, 602-603
pwd command, 175
redundant interfaces, 16, 84-87
regular expression operators, 46
regular expressions (regex)
ASDM (Adaptive Security Device Manager), 533
configuring, 525-526
metacharacters, 524-525
reloading, ASA (Adaptive Security Appliances), 34, 63-70
remote access VPNs, 16
remote accounting, AAA (Authentication, Authorization, and Accounting), configuring, 222-223
remote management access
configuring, 188-189
HTTPS, 194
Telnet, 190-192
SSH, configuring, 192-194
troubleshooting, 230-231
removing, Security Contexts, 663
rename command, 173
renaming, files, 62-173
Reputation-based Botnet Traffic Filtering, firewalls, 15
resource classes, creating, 663-665
resource management
configuring, 663-665
verifying, 665
RIPv2, routing, 132-135
rmdir command, 174
roles, failover, 675-681
ROMMON mode (CLI), 41
route lookup (CLI), 41
routed firewall mode, 632
versus transparent firewall mode, 635
routing
asymmetric, detecting, 703-705
EIGRP (Enhanced Interior Gateway Routing Protocol), 135-142
queues, traffic, 612-616
OSPF (Open Shortest Path First), 142-153
RIPv2, 132-135
static, configuring, 124-132
routing information, 122-124
routing tables, verifying, 151
RSA key pairs, creating default, 192
rule priority, NAT (Network Address Translation), 330, 340
rules, access control, default, 410-411

searching, command output, 45-47
Security Contexts, 654-655
  configuring, 658-661
  creating, 659-661
  editing, 663
  managing, 661-663
  resource management, configuring, 663-665
  troubleshooting, 665-666
  verifying, 661
security domains
  firewalls, 8-10
  physical separation, 10
security levels, interfaces, 408
  configuring, 100-104
security parameters, interfaces, configuring, 98-104
security policies, ASDM (Adaptive Security Device Manager), creating in, 490-495
Security Service Modules (SSMs). See SSMs (Security Service Modules)
self-signed certificates, creating, 194
servers, syslog, 265-267
session auditing, firewalls, 15

session logging
  configuring, 255-271
  implementing, 272-273
  managing, 252-255
  troubleshooting, 273-274
  verifying, 271-273
settings, devices, 165-168
severity levels, messages, 255
shaping traffic, 617
  configuring, 621-624
show access-list brief command, 434
show access-list command, 433-452
show clock command, 251-432
show conn command, 400
show conn detail command, 400
show context command, 661
show failover command, 706-708
show interface command, 107
show interface ip brief command, 108
show local-host command, 404
show nat detail command, 382
show port-channel summary command, 94
show route command, 152
show running-config access-list command, 451
show shun command, 456
show version command, 705
show xlate command, 311-312
show xlate detail command, 324
shun command, 456
shunning packets, 455-457
site-to-site VPNs, 16
SNMP (Simple Network Management Protocol), 253
  monitoring, configuring, 225-229
  user information, adding, 228
software, managing, 176-186
SPF (stateful packet filtering)
  engines, firewalls, 15
  firewalls, 12-13
spoofing attacks, transparent firewall mode, 642
SSH (secure shell), remote access, configuring, 192-194
SSMs (Security Service Modules), 22-25, 718-721
AIP (Advanced Inspection and Prevention), 22-23, 715
AIP-SSM (Advanced Inspection and Prevention Security Services Module)
  configuring, 723-724
  initializing, 723
  installing, 721-724
CSC (Content Security and Control), 23
CSC-SSM (Content Security and Control Security Service Module), 719-720
  integration, 724-725
deployment, 719
firewalls, 15
4GE (4-port Gigabit Ethernet), 24
inline operation, 720
module components, 718-719
promiscuous operation, 721
state tables, 397-409
  connection tables, 398-401
  inbound/outbound, 403
  inside/outside, 403
  local host tables, 403-404
  logging, 405
stateful filtering, 406-408
stateful packet filtering, firewalls, 12-15
statefully tracked protocol information, 398
stateless packet filtering, 11-12
static identity NAT, configuring, 326-328
static inside NAT
  configuring, 312-315
  verifying, 323-324
static inside PAT, configuring, 317-320
static inside policy NAT, configuring, 320-323
static NAT, 295
  comparing configurations, 351-352
static PAT, 295
static port translations, configuring, auto NAT, 349-351
static routes, displaying, 152
static routing, configuring, 124-132
syslog messages
  examining, 457-459
NAT (Network Address Translation), 338
syslog servers, 265-267
system time
  configuring, 247-252
NTP, 249-252
T

tables
  NAT (Network Address Translation), 341-343
  routing, verification, 151
  state, 397-409
TCP (Transport Control Protocol), 398
  connections, flags, 401-402
  normalization, inspecting, 499-504
  parameters, inspecting, 499-504
Telnet, remote access, configuring, 190-192
terminal screen format, CLI (command line interface), 47
testing
  network connectivity, 733-736
  Testing AAA Authentication, 214
  threat detection, 570-578
time-based access rules, 427-432
timeouts, authentication, configuring, 598
timers, failover, configuring, 701-702
TLS proxy, 603
tracert command, 736
tracking, static routes, 126-132
traffic
  bandwidth, controlling, 616-624
  handling, fragmented, 610-611
  inspecting, 465-472
    botnet traffic, 561-570
    dynamic protocols, 507-516
    MPF (Modular Policy Framework), 479-483
    OSI Layers 3-4, 484-506
    OSI Layers 5-7, 517-561
  threat detection, 570-578
performance, ASA models, 25-29
policing, 617, 618-621
policy maps, effects, 490
prioritizing, 612-616
shaping, 617
  configuring, 621-624
transparent firewall mode, controlling in, 639-642
virtualization, 17
traffic analysis tools, 726-729
  Packet Capture, 742-761
  Packet Tracer, 737-742
  ping command, 733-735
traffic correlation, firewalls, 16
traffic policers, configuring, 618-621
translations, NAT (Network Address Translation), 373-375
transparent firewall mode, 626-628-633
  ARP (Address Resolution Protocol), 642-645
  bridge groups, 634
  configuring, 635-639
  controlling traffic in, 639-642
  MAC address learning, disabling, 645-647
  versus routed firewall mode, 635
troubleshooting
  access control, 457-463
  event logging, 273-274
  remote management access, 230-231
  Security Contexts, 665-666
  session logging, 273-274
  user-based proxy, 602-603
trunk lists, configuring, 96
tuning
  failover, 701-706
  Layer 3-4 connection limits, 495-499
  NAT (Network Address Translation), 380-381
twice NAT, configuring, 370-373

UC (Unified Communication) proxy, firewalls, 16
UDP (user datagram protocol), 398
Unicast Reverse Path Forwarding (uRPF), 454-455
unidirectional manual static NAT, configuring, 376-377
unified telepresence, proxy services, 603
UN-NAT (Packet Tracer), 737
uRPF (Unicast Reverse Path Forwarding), 454-455
user authentication
configuring, 591-600
user-based proxy, 586-587
verifying, 595
user EXEC mode (CLI), 40
user information, SNMP, adding, 228
user session accounting, configuring, 601-602
user-based access control, firewalls, 15
user-based proxy, 586-589
configuring, 591
preconfiguration, 588-589
troubleshooting, 602-603
UTC (Coordinated Universal Time), 247

V-Z

verification
access control, 454-457
auto NAT, 361-363
event logging, 271-273
failover, 706-708
interface access rules, 432-438
interface operations, 107-109
object groups, 450-453
resource management, 665
routing tables, 151
Security Contexts, 661
session logging, 271-273
user authentication, 595

virtual firewalls
configuring, 658
creating, 649-651, 654-656
deployment, 656-658
managing, 661-663
packet classification, 655-656
resource management
configuring, 663-665
verifying, 665
Security Contexts, 654-655
configuring, 658-661
troubleshooting, 665-666
verifying, 661
virtual HTTP, 590
virtual HTTP servers, configuring, 595
virtual reassembly, displaying active, 612
virtualization, 654-656
policies, 17
traffic, 17
virtualization licenses (ASA), 31
VLANs (virtual LANs), interfaces, configuring, 95-98
VPNs (virtual private networks)
remote access, 16
site-to-site, 16