



SECURITY

## Cisco ASA

All-in-One Firewall, IPS, and VPN Adaptive  
Security Appliance

Third Edition

[ciscopress.com](http://ciscopress.com)

Jazib Frahim, CCIE® No. 5459  
Omar Santos

FREE SAMPLE CHAPTER



SHARE WITH OTHERS

# Cisco ASA

---

All-in-One Next-Generation Firewall, IPS, and VPN  
Services, Third Edition

Jazib Frahim, CCIE No. 5459

Omar Santos

Andrew Ossipov, CCIE No. 18483

**Cisco Press**

800 East 96th Street

Indianapolis, IN 46240

# Cisco ASA: All-in-One Next-Generation Firewall, IPS, and VPN Services, Third Edition

Jazib Frahim, Omar Santos, Andrew Ossipov

Copyright © 2014 Pearson Education, Inc.

Published by:

Cisco Press

800 East 96th Street

Indianapolis, IN 46240 USA

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from the publisher, except for the inclusion of brief quotations in a review.

Printed in the United States of America

Second Printing September 2014

Library of Congress Control Number: 2014936118

ISBN-13: 978-1-58714-307-6

ISBN-10: 1-58714-307-0

## Warning and Disclaimer

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

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

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

## Trademark Acknowledgments

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

## Special Sales

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at [corpsales@pearsoned.com](mailto:corpsales@pearsoned.com) or (800) 382-3419.

For government sales inquiries, please contact [governmentsales@pearsoned.com](mailto:governmentsales@pearsoned.com).

For questions about sales outside the U.S., please contact [international@pearsoned.com](mailto:international@pearsoned.com).

## Feedback Information

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

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

We greatly appreciate your assistance.

<b>Publisher:</b> Paul Boger	<b>Business Operation Manager, Cisco Press:</b> Jan Cornelssen
<b>Associate Publisher:</b> Dave Dusthimer	<b>Executive Editor:</b> Brett Bartow
<b>Technical Editors:</b> Magnus Mortensen, Phillip Strelau	<b>Managing Editor:</b> Sandra Schroeder
<b>Development Editor:</b> Marianne Bartow	<b>Project Editor:</b> Seth Kerney
<b>Copy Editor:</b> Bill McManus	<b>Book Designer:</b> Louisa Adair
<b>Editorial Assistant:</b> Vanessa Evans	<b>Composition:</b> Trina Wurst
<b>Indexer:</b> Brad Herriman	<b>Proofreader:</b> Sarah Kearns



**Americas Headquarters**  
Cisco Systems, Inc.  
San Jose, CA

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

**Europe Headquarters**  
Cisco Systems International BV  
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSF, COOP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, Gigaset, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0812R)

## About the Authors

**Jazib Frahim**, CCIE No. 5459, is a Principal Engineer in the Global Security Services Practice at Cisco. He has been with Cisco for over 15 years, with a focus on cyber-security and emerging security technologies. Jazib is also responsible for guiding customers in the design and implementation of security solutions and technologies in their networks with a focus on network security. He leads a team of solutions architects to guide them through the lifecycle of services and solutions development. Jazib has also been engaged in the development of a number of customer-focused services, such as managed threat defense, network-based identity, bring-your-own-device (BYOD), and many others.

Jazib holds a bachelor's degree in computer engineering from Illinois Institute of Technology and a master's degree in business administration (MBA) from North Carolina State University.

In addition to CISSP, Jazib also holds two CCIEs, one in routing and switching and the other in security. He has presented at many industry events, such as Cisco Live, Interop, and ISSA, on multiple occasions. He has also authored and coauthored numerous technical documents, whitepapers, and books, including the following Cisco Press titles:

- *Cisco ASA: All-in-One Firewall, IPS, and VPN Adaptive Security Appliance*
- *Cisco ASA: All-in-One Firewall, IPS, Anti-X, and VPN Adaptive Security Appliance*, Second Edition
- *Cisco Network Admission Control, Volume II: NAC Deployment and Troubleshooting*
- *SSL Remote Access VPNs*

**Omar Santos** is a Senior Incident Manager of Cisco's Product Security Incident Response Team (PSIRT), where he mentors and leads engineers and incident managers during the investigation and resolution of security vulnerabilities in all Cisco products. Omar has designed, implemented, and supported numerous secure networks for Fortune 500 companies and the U.S. government. Prior to his current role, he was a technical leader within the World Wide Security Practice and Cisco's Technical Assistance Center (TAC), where he taught, led, and mentored many engineers within both organizations.

Omar is an active member of the security community, where he leads several industry-wide initiatives and standards bodies. His active role helps businesses, academic institutions, state and local law enforcement agencies, and other participants that are dedicated to increasing the security of the critical infrastructure.

Omar has delivered numerous technical presentations at conferences and to Cisco customers and partners, as well as many C-level executive presentations to many organizations. He has authored numerous whitepapers, articles, and security configuration guidelines and best practices, and has also authored or coauthored the following Cisco Press books:

- *Cisco ASA: All-in-One Firewall, IPS, and VPN Adaptive Security Appliance*
- *Cisco ASA: All-in-One Firewall, IPS, Anti-X, and VPN Adaptive Security Appliance*, Second Edition

- *Cisco Network Admission Control, Volume II: NAC Deployment and Troubleshooting*
- *End-to-End Network Security: Defense-in-Depth*

**Andrew Ossipov**, CCIE No. 18483 and CISSP No. 344324, is currently a Technical Marketing Engineer at Cisco with primary concentration on firewall, intrusion prevention, and other Cisco Data Center Security solutions. With over 15 years of networking experience, Andrew previously worked with LAN switching, routing protocol, and network data storage technologies and performed academic research in the area of VoIP. At Cisco, Andrew is involved in a broad range of activities that include solving customers' technical problems of the highest complexity, architecting features and products, and defining the future direction of the product portfolio. He is an inventor and co-inventor of multiple pending cross-technology patents. Andrew received his bachelor of science in computer engineering and master of science in electrical engineering degrees from Wichita State University.

## About the Technical Reviewers

**Magnus Mortensen**, CCIE No. 28219, has more than 10 years of network experience and has been employed at Cisco since June of 2006. During his years at Cisco, Magnus has been working with firewall and network security technologies and is currently part of the Security & NMS Technical Leadership team. Based in Research Triangle Park, North Carolina, Magnus specializes in the full breadth of firewall technologies and is one of the founding members of the Cisco TAC Security Podcast Series. Besides troubleshooting customer networks, he enjoys creating new tools and programs that help advance not only TAC, but Cisco as an organization. Originally from southern New York state, Magnus moved down to North Carolina after graduating from Rensselaer Polytechnic Institute with a bachelor's degree in computer systems engineering.

**Phillip Strelau** has been with Cisco Systems since 2008 and is a technical lead on the Firewall Technical Assistance Center (TAC) team. He graduated from Rochester Institute of Technology with a degree in network security and systems administration and has worked in the networking field for almost a decade. During his time at Cisco, Phillip has worked with product developers to enhance the ASA, CX, IPS, and CSM product lines. He is also active in the Cisco Certification space, helping to provide content and feedback for CCNA Security and CCNP Security, and having helped to create the Cisco Cybersecurity Specialist certification.

## Dedications

### **Jazib Frahim:**

I would like to dedicate this book to my lovely wife, Sadaf, and my two lovely and adorable children, Zayan and Zeenia, who have patiently put up with me during the writing process.

I would also like to dedicate this book to my parents, Frahim and Perveen, who support and encourage me in all my endeavors.

Finally, I would like to thank my siblings, including my brother Shazib and sisters Erum and Sana, sister-in-law Asiya, brother-in-law Faraz, my cute nephew Shayan, and my adorable nieces Shiza and Alisha. Thank you for your patience and understanding during the development of this book.

### **Omar Santos:**

I would like to dedicate this book to my lovely wife, Jeannette, and my two beautiful children, Hannah and Derek, who have inspired and supported me throughout the development of this book.

I also dedicate this book to my father, Jose; and in memory of my mother, Generosa. Without their knowledge, wisdom, and guidance, I would not have the goals that I strive to achieve today.

### **Andrew Ossipov:**

I dedicate this book to my parents, Liudmila and Evgeny, whose never ending love, care, and wisdom continue to be the foundation of everything that I am today and something for which I will be forever grateful. I also dedicate this to my sister, Polina, who always stays by my side and constantly humbles me by asking for advice despite being one of the smartest people that I know.

This work would not be possible without the love, support, and inspiration of my precious wife, Oksana, who put up with the long evening and weekend hours to ensure the timely completion of my chapters.

I would also like to recognize my Cisco managers, Hari Tewari and Arshad Saeed, who were extremely supportive over the course of this project.

## Acknowledgments

We would like to thank the technical editors, Magnus Mortensen and Phillip Strelau, for their time and technical expertise. They verified our work and corrected us in all the major and minor mistakes that were hard to find.

We would like to thank the Cisco Press team, especially Brett Bartow, Marianne Bartow, Christopher Cleveland, and Andrew Cupp, for their patience, guidance, and consideration. Their efforts are greatly appreciated.

Many thanks to our Cisco management team, including Bryan Palma, David Phillips, Sanjay Pol, Klee Michaelis, and Russell Smoak, for their continuous support. They highly encouraged us throughout this project.

Kudos to the Cisco ASA product development team for delivering such a great product. Their support is also greatly appreciated during the development of this book.

Finally, we would like to acknowledge the Cisco TAC. Some of the best and brightest minds in the networking industry work there, supporting our Cisco customers often under very stressful conditions and working miracles daily. They are truly unsung heroes, and we are all honored to have had the privilege of working side by side with them in the trenches of the TAC.



## Contents at a Glance

	Introduction	
Chapter 1	Introduction to Security Technologies	1
Chapter 2	Cisco ASA Product and Solution Overview	29
Chapter 3	Licensing	59
Chapter 4	Initial Setup	81
Chapter 5	System Maintenance	119
Chapter 6	Cisco ASA Services Module	173
Chapter 7	Authentication, Authorization, and Accounting (AAA) Services	191
Chapter 8	Controlling Network Access: The Traditional Way	229
Chapter 9	Implementing Next-Generation Firewall Services with ASA CX	267
Chapter 10	Network Address Translation	337
Chapter 11	IPv6 Support	379
Chapter 12	IP Routing	391
Chapter 13	Application Inspection	465
Chapter 14	Virtualization	531
Chapter 15	Transparent Firewalls	591
Chapter 16	High Availability	641
Chapter 17	Implementing Cisco ASA Intrusion Prevention System (IPS)	733
Chapter 18	Tuning and Monitoring IPS	787
Chapter 19	Site-to-Site IPsec VPNs	801
Chapter 20	IPsec Remote-Access VPNs	859
Chapter 21	Configuring and Troubleshooting PKI	931
Chapter 22	Clientless Remote-Access SSL VPNs	979
Chapter 23	Client-Based Remote-Access SSL VPNs	1085
Chapter 24	IP Multicast Routing	1119
Chapter 25	Quality of Service	1131
	Index	1165

# Contents

Introduction

## **Chapter 1 Introduction to Security Technologies 1**

Firewalls 2

Network Firewalls 2

*Packet-Filtering Techniques* 2

*Application Proxies* 3

*Network Address Translation* 3

*Stateful Inspection Firewalls* 6

Demilitarized Zones (DMZ) 7

Deep Packet Inspection 8

Next-Generation Context-Aware Firewalls 8

Personal Firewalls 9

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) 9

Pattern Matching and Stateful Pattern-Matching Recognition 11

Protocol Analysis 12

Heuristic-Based Analysis 12

Anomaly-Based Analysis 12

Global Threat Correlation Capabilities 14

Virtual Private Networks 14

Technical Overview of IPsec 16

*IKEv1 Phase 1* 16

*IKEv1 Phase 2* 20

*IKEv2* 23

SSL VPNs 23

Cisco AnyConnect Secure Mobility 25

Cloud and Virtualization Security 26

## **Chapter 2 Cisco ASA Product and Solution Overview 29**

Cisco ASA Model Overview 30

Cisco ASA 5505 Model 31

Cisco ASA 5510 Model 35

Cisco ASA 5512-X Model 38

Cisco ASA 5515-X Model 40

Cisco ASA 5520 Model 41

Cisco ASA 5525-X Model 42

Cisco ASA 5540 Model 43

Cisco ASA 5545-X Model 44

Cisco ASA 5550 Model 45

Cisco ASA 5555-X Model 46

Cisco ASA 5585-X Models	47
Cisco Catalyst 6500 Series ASA Services Module	51
Cisco ASA 1000V Cloud Firewall	52
Cisco ASA Next-Generation Firewall Services (Formerly Cisco ASA CX)	53
Cisco ASA AIP-SSM Module	53
Cisco ASA AIP-SSM-10	54
Cisco ASA AIP-SSM-20	54
Cisco ASA AIP-SSM-40	54
Cisco ASA Gigabit Ethernet Modules	55
Cisco ASA SSM-4GE	55
Cisco ASA 5580 Expansion Cards	56
Cisco ASA 5500-X Series 6-Port GE Interface Cards	57

### **Chapter 3 Licensing 59**

Licensed Features on ASA	59
Basic Platform Capabilities	61
Advanced Security Features	63
Tiered Capacity Features	65
Displaying License Information	66
Managing Licenses with Activation Keys	68
Permanent and Time-Based Activation Keys	68
<i>Combining Keys</i>	69
<i>Time-Based Key Expiration</i>	70
Using Activation Keys	71
Combined Licenses in Failover and Clustering	73
License Aggregation Rules	73
Aggregated Time-Based License Countdown	75
Shared Premium VPN Licensing	75
Shared Server and Participants	76
<i>Shared License</i>	76
<i>Shared Licensing Operation</i>	76
Configuring Shared Licensing	78
<i>Licensing Server</i>	78
<i>Participants</i>	79
<i>Backup Licensing Server</i>	79
<i>Monitoring Shared Licensing Operation</i>	80

### **Chapter 4 Initial Setup 81**

Accessing the Cisco ASA Appliances	81
Establishing a Console Connection	82
Command-Line Interface	85
Managing Licenses	87

Initial Setup	90
Initial Setup via CLI	90
Initial Setup of ASDM	92
<i>Uploading ASDM</i>	92
<i>Setting Up the Appliance</i>	93
<i>Accessing ASDM</i>	94
<i>Functional Screens of ASDM</i>	97
Device Setup	100
Setting Up a Device Name and Passwords	100
Configuring an Interface	102
<i>Configuring a Data-Passing Interface</i>	102
<i>Configuring a Subinterface</i>	106
<i>Configuring an EtherChannel Interface</i>	109
<i>Configuring a Management Interface</i>	111
DHCP Services	112
Setting Up the System Clock	114
Manual Clock Adjustment	114
<i>Time Zone</i>	114
<i>Date</i>	116
<i>Time</i>	116
Automatic Clock Adjustment Using the Network Time Protocol	116
<b>Chapter 5 System Maintenance</b>	<b>119</b>
Configuration Management	119
Running Configuration	119
Startup Configuration	123
Removing the Device Configuration	124
Remote System Management	126
Telnet	126
Secure Shell (SSH)	129
System Maintenance	132
Software Installation	132
<i>Image Upgrade via Cisco ASDM</i>	132
<i>Image Upgrade via the Cisco ASA CLI</i>	133
<i>Image Upload Using ROMMON</i>	136
Password Recovery Process	137
Disabling the Password Recovery Process	141
System Monitoring	144
System Logging	144
<i>Enabling Logging</i>	146
<i>Defining Event List</i>	147

	<i>Logging Types</i>	149
	<i>Defining a Syslog Server</i>	153
	<i>Defining an Email Server</i>	154
	<i>Storing Logs Internally and Externally</i>	154
	<i>Syslog Message ID Tuning</i>	156
	NetFlow Secure Event Logging (NSEL)	156
	<i>Step 1: Define a NetFlow Collector</i>	157
	<i>Step 2: Define a NetFlow Export Policy</i>	159
	Simple Network Management Protocol (SNMP)	160
	<i>Configuring SNMP</i>	161
	<i>SNMP Monitoring</i>	164
	Device Monitoring and Troubleshooting	165
	CPU and Memory Monitoring	165
	Troubleshooting Device Issues	168
	<i>Troubleshooting Packet Issues</i>	168
	<i>Troubleshooting CPU Issues</i>	172
<b>Chapter 6</b>	<b>Cisco ASA Services Module</b>	<b>173</b>
	Cisco ASA Services Module Overview	173
	Hardware Architecture	174
	Host Chassis Integration	175
	Managing Host Chassis	176
	Assigning VLAN Interfaces	177
	Monitoring Traffic Flow	178
	Common Deployment Scenarios	180
	Internal Segment Firewalling	181
	Edge Protection	182
	Trusted Flow Bypass with Policy Based Routing	183
	Traffic Flow	185
	Sample PBR Configuration	185
<b>Chapter 7</b>	<b>Authentication, Authorization, and Accounting (AAA) Services</b>	<b>191</b>
	AAA Protocols and Services Supported by Cisco ASA	192
	RADIUS	194
	TACACS+	195
	RSA SecurID	196
	Microsoft Windows NTLM	197
	Active Directory and Kerberos	197
	Lightweight Directory Access Protocol	197
	Defining an Authentication Server	198
	Configuring Authentication of Administrative Sessions	204
	Authenticating Telnet Connections	204

Authenticating SSH Connections	206
Authenticating Serial Console Connections	207
Authenticating Cisco ASDM Connections	208
Authenticating Firewall Sessions (Cut-Through Proxy Feature)	209
Authentication Timeouts	214
Customizing Authentication Prompts	214
Configuring Authorization	215
Command Authorization	217
Configuring Downloadable ACLs	218
Configuring Accounting	219
RADIUS Accounting	220
TACACS+ Accounting	221
Troubleshooting Administrative Connections to Cisco ASA	222
Troubleshooting Firewall Sessions (Cut-Through Proxy)	225
ASDM and CLI AAA Test Utility	226
<b>Chapter 8 Controlling Network Access: The Traditional Way</b>	<b>229</b>
Packet Filtering	229
Types of ACLs	232
<i>Standard ACLs</i>	233
<i>Extended ACLs</i>	233
<i>EtherType ACLs</i>	233
<i>Webtype ACLs</i>	234
Comparing ACL Features	234
Through-the-Box-Traffic Filtering	235
To-the-Box-Traffic Filtering	240
Advanced ACL Features	243
Object Grouping	243
<i>Object Types</i>	243
<i>Configuration of Object Types</i>	245
<i>Object Grouping and ACLs</i>	248
Standard ACLs	250
Time-Based ACLs	251
Downloadable ACLs	254
ICMP Filtering	254
Deployment Scenario for Traffic Filtering	255
Using ACLs to Filter Inbound Traffic	255
<i>Configuration Steps with ASDM</i>	257
<i>Configuration Steps with CLI</i>	259
Monitoring Network Access Control	260
Monitoring ACLs	260

**Chapter 9 Implementing Next-Generation Firewall Services with ASA CX 267**

- CX Integration Overview 268
  - Logical Architecture 269
  - Hardware Modules 270
  - Software Modules 271
  - High Availability 272
- ASA CX Architecture 273
  - Data Plane 274
  - Eventing and Reporting 275
  - User Identity 275
  - TLS Decryption Proxy 276
  - HTTP Inspection Engine 276
  - Application Inspection Engine 276
  - Management Plane 276
  - Control Plane 276
- Preparing ASA CX for Configuration 277
- Managing ASA CX with PRSM 282
  - Using PRSM 283
  - Configuring User Accounts 286
  - CX Licensing 288
  - Component and Software Updates 290
  - Signatures and Engines* 290
  - System Software* 291
  - Configuration Database Backup 292
- Defining CX Policy Elements 293
  - Network Groups 295
  - Identity Objects 296
  - URL Objects 298
  - User Agent Objects 299
  - Application Objects 299
  - Secure Mobility Objects 300
  - Interface Roles 301
  - Service Objects 302
  - Application-Service Objects 303
  - Source Object Groups 304
  - Destination Object Groups 305
  - File Filtering Profiles 306
  - Web Reputation Profiles 306
  - NG IPS Profiles 307
- Enabling User Identity Services 309

Configuring Directory Servers	310
Connecting to AD Agent or CDA	312
Tuning Authentication Settings	313
Defining User Identity Discovery Policy	314
Enabling TLS Decryption	316
Configuring Decryption Settings	318
Defining a Decryption Policy	320
Enabling NG IPS	323
Defining Context-Aware Access Policies	324
Configuring ASA for CX Traffic Redirection	327
Monitoring ASA CX	329
Dashboard Reports	329
Connection and System Events	331
Packet Captures	332

## **Chapter 10 Network Address Translation 337**

Types of Address Translation	338
Network Address Translation	338
Port Address Translation	340
Address Translation Methods	341
Static NAT/PAT	341
Dynamic NAT/PAT	343
Policy NAT/PAT	344
Identity NAT	344
Security Protection Mechanisms Within Address Translation	345
Randomization of Sequence Numbers	345
TCP Intercept	346
Understanding Address Translation Behavior	346
Address Translation Behavior Prior to Version 8.3	346
<i>Packet Flow Sequence in Pre-8.3 Version</i>	347
<i>NAT Order of Operation for Pre-8.3 Versions</i>	348
Redesigning Address Translation (Version 8.3 and Later)	349
<i>NAT Modes in Version 8.3 and Later</i>	349
<i>NAT Order of Operation for Version 8.3 and Later</i>	350
Configuring Address Translation	350
Auto NAT Configuration	351
<i>Available Auto NAT Settings</i>	351
<i>Auto NAT Configuration Example</i>	353
Manual NAT Configuration	356
<i>Available Manual NAT Settings</i>	356
<i>Manual NAT Configuration Example</i>	357



	Integrating ACLs and NAT	359
	<i>Pre-8.3 Behavior for NAT and ACL Integration</i>	359
	<i>Behavior of NAT and ACL Integration in Version 8.3 and Later</i>	361
	Configuration Use Cases	362
	<i>Use Case 1: Dynamic PAT for Inside Network with Static NAT for a DMZ Web Server</i>	363
	<i>Use Case 2: Static PAT for a Web Server Located on the DMZ Network</i>	364
	<i>Use Case 3: Static NAT for Overlapping Subnets Using Twice NAT</i>	366
	<i>Use Case 4: Identity NAT for Site-to-Site VPN Tunnel</i>	367
	<i>Use Case 5: Dynamic PAT for Remote-Access VPN Clients</i>	369
	DNS Doctoring	372
	Monitoring Address Translations	375
<b>Chapter 11</b>	<b>IPv6 Support</b>	<b>379</b>
	IP Version 6 Introduction	379
	IPv6 Header	380
	Supported IPv6 Address Types	381
	<i>Global Unicast Address</i>	382
	<i>Site-Local Address</i>	382
	<i>Link-Local Address</i>	382
	Configuring IPv6	382
	IP Address Assignment	383
	IPv6 DHCP Relay	384
	Optional IPv6 Parameters	385
	<i>Neighbor Solicitation Messages</i>	385
	<i>Neighbor Reachable Time</i>	385
	<i>Router Advertisement Transmission Interval</i>	385
	Setting Up an IPv6 ACL	386
	IPv6 Address Translation	389
<b>Chapter 12</b>	<b>IP Routing</b>	<b>391</b>
	Configuring Static Routes	392
	Static Route Monitoring	395
	Displaying the Routing Table	399
	RIP	400
	Configuring RIP	401
	RIP Authentication	403
	RIP Route Filtering	406
	Configuring RIP Redistribution	409
	Troubleshooting RIP	409
	<i>Scenario 1: RIP Version Mismatch</i>	410

<i>Scenario 2: RIP Authentication Mismatch</i>	411
<i>Scenario 3: Multicast or Broadcast Packets Blocked</i>	411
OSPF	412
Configuring OSPF	413
<i>Enabling OSPF</i>	414
OSPF Virtual Links	419
Configuring OSPF Authentication	422
Configuring OSPF Redistribution	426
Stub Areas and NSSAs	428
OSPF Type 3 LSA Filtering	429
OSPF neighbor Command and Dynamic Routing over a VPN Tunnel	431
OSPFv3	433
Troubleshooting OSPF	433
<i>Useful Troubleshooting Commands</i>	433
<i>Mismatched Areas</i>	440
<i>OSPF Authentication Mismatch</i>	440
<i>Troubleshooting Virtual Link Problems</i>	440
EIGRP	441
Configuring EIGRP	441
<i>Enabling EIGRP</i>	441
<i>Configuring Route Filtering for EIGRP</i>	445
<i>EIGRP Authentication</i>	447
<i>Defining Static EIGRP Neighbors</i>	448
<i>Route Summarization in EIGRP</i>	448
<i>Split Horizon</i>	450
<i>Route Redistribution in EIGRP</i>	450
<i>Controlling Default Information</i>	453
Troubleshooting EIGRP	454
<i>Useful Troubleshooting Commands</i>	454
<i>Scenario 1: Link Failures</i>	458
<i>Scenario 2: Misconfigured Hello and Hold Intervals</i>	459
<i>Scenario 3: Misconfigured Authentication Parameters</i>	462
<b>Chapter 13 Application Inspection</b>	<b>465</b>
Enabling Application Inspection	468
Selective Inspection	469
CTIQBE Inspection	473
DCERPC Inspection	476
DNS Inspection	476
ESMTP Inspection	481
File Transfer Protocol	484

General Packet Radio Service Tunneling Protocol	486
GTPv0	487
GTPv1	489
Configuring GTP Inspection	490
H.323	492
H.323 Protocol Suite	493
H.323 Version Compatibility	495
Enabling H.323 Inspection	496
Direct Call Signaling and Gatekeeper Routed Control Signaling	499
T.38	499
Cisco Unified Communications Advanced Support	499
Phone Proxy	500
TLS Proxy	505
Mobility Proxy	506
Presence Federation Proxy	506
HTTP	507
Enabling HTTP Inspection	507
<i>strict-http</i> Command	510
<i>content-length</i> Command	510
<i>content-type-verification</i> Command	511
<i>max-header-length</i> Command	511
<i>max-uri-length</i> Command	512
<i>port-misuse</i> Command	512
<i>request-method</i> Command	513
<i>transfer-encoding type</i> Command	515
ICMP	515
ILS	516
Instant Messenger (IM)	517
IPsec Pass-Through	518
MGCP	519
NetBIOS	521
PPTP	522
Sun RPC	522
RSH	523
RTSP	523
SIP	524
Skinny (SCCP)	525
SNMP	527
SQL*Net	528
TFTP	528

WAAS 528  
 XDMCP 529

## **Chapter 14 Virtualization 531**

Architectural Overview 533  
     System Execution Space 533  
     Admin Context 535  
     User Context 535  
     Packet Classification 538  
     *Packet Classification Criteria* 538  
     *Destination IP Address* 539  
     *Unique MAC Address* 540  
     Packet Flow in Multiple Mode 541  
     *Forwarding Without a Shared Interface* 541  
     *Forwarding with a Shared Interface* 542  
 Configuration of Security Contexts 544  
     Step 1: Enable Multiple Security Contexts Globally 544  
     Step 2: Set Up the System Execution Space 547  
     Step 3: Configure Interfaces 549  
     Step 4: Specify a Configuration URL 550  
     Step 5: Configure an Admin Context 552  
     Step 6: Configure a User Context 553  
     Step 7: Manage the Security Contexts (Optional) 554  
     Step 8: Resource Management (Optional) 555  
     *Step 1: Define a Resource Class* 556  
     *Step 2: Map the Resource Class to a Context* 558  
 Deployment Scenarios 559  
     Virtual Firewall with Non-Shared Interfaces 559  
     *Configuration Steps with ASDM* 561  
     *Configuration Steps with CLI* 569  
     Virtual Firewall with a Shared Interface 572  
     *Configuration Steps with ASDM* 574  
     *Configuration Steps Using CLI* 582  
 Monitoring and Troubleshooting the Security Contexts 586  
     Monitoring 586  
     Troubleshooting 588  
     *Security Contexts Are Not Added* 588  
     *Security Contexts Are Not Saved on the Local Disk* 588  
     *Security Contexts Are Not Saved on the FTP Server* 589  
     *User Having Connectivity Issues When Shared Security Contexts Are Used* 590

## **Chapter 15 Transparent Firewalls 591**

Architectural Overview	594
Single-Mode Transparent Firewalls	594
<i>Packet Flow in an SMTF</i>	595
Multimode Transparent Firewalls	597
<i>Packet Flow in an MMTF</i>	597
Restrictions When Using Transparent Firewalls	599
Transparent Firewalls and VPNs	599
Transparent Firewalls and NAT	600
Configuration of Transparent Firewalls	602
Configuration Guidelines	602
Configuration Steps	603
<i>Step 1: Enable Transparent Firewalls</i>	603
<i>Step 2: Set Up Interfaces</i>	604
<i>Step 3: Configure an IP Address</i>	605
<i>Step 4: Set Up Routes</i>	606
<i>Step 5: Configure Interface ACLs</i>	608
<i>Step 6: Configure NAT (Optional)</i>	611
<i>Step 7: Add Static L2F Table Entries (Optional)</i>	612
<i>Step 8: Enable ARP Inspection (Optional)</i>	613
<i>Step 9: Modify L2F Table Parameters (Optional)</i>	615
Deployment Scenarios	616
SMTF Deployment	617
<i>Configuration Steps Using ASDM</i>	618
<i>Configuration Steps Using CLI</i>	622
MMTF Deployment with Security Contexts	623
<i>Configuration Steps Using ASDM</i>	625
<i>Configuration Steps Using CLI</i>	632
Monitoring and Troubleshooting Transparent Firewalls	636
Monitoring	636
Troubleshooting	637
Hosts Are Not Able to Communicate	637
Moved Host Is Not Able to Communicate	639
General Syslogging	640

## **Chapter 16 High Availability 641**

Redundant Interfaces	642
Using Redundant Interfaces	642
Deployment Scenarios	643
Configuration and Monitoring	644
Static Route Tracking	646

Configuring Static Routes with an SLA Monitor	647
Floating Connection Timeout	649
Sample Backup ISP Deployment	649
Failover	652
Unit Roles and Functions in Failover	652
Stateful Failover	653
Active/Standby and Active/Active Failover	654
Failover Hardware and Software Requirements	656
<i>Zero Downtime Upgrade in Failover</i>	657
<i>Failover Licensing</i>	658
Failover Interfaces	658
<i>Stateful Link</i>	659
<i>Failover Link Security</i>	659
<i>Data Interface Addressing</i>	660
<i>Asymmetric Routing Groups</i>	662
Failover Health Monitoring	664
State and Role Transition	666
Configuring Failover	667
<i>Basic Failover Settings</i>	668
<i>Data Interface Configuration</i>	671
<i>Failover Policies and Timers</i>	673
<i>Active/Active Failover</i>	674
Monitoring and Troubleshooting Failover	678
Active/Standby Failover Deployment Scenario	680
Clustering	685
Unit Roles and Functions in Clustering	685
<i>Master and Slave Units</i>	685
<i>Flow Owner</i>	686
<i>Flow Director</i>	686
<i>Flow Forwarder</i>	687
Clustering Hardware and Software Requirements	687
<i>Zero Downtime Upgrade in Clustering</i>	688
<i>Unsupported Features</i>	689
<i>Cluster Licensing</i>	690
Control and Data Interfaces	690
<i>Spanned EtherChannel Mode</i>	693
<i>Individual Mode</i>	695
<i>Cluster Management</i>	697
Cluster Health Monitoring	697
Network Address Translation	698
Performance	700

	<i>Centralized Features</i>	701
	<i>Scaling Factors</i>	701
	Packet Flow	702
	<i>TCP Connection Processing</i>	702
	<i>UDP Connection Processing</i>	703
	<i>Centralized Connection Processing</i>	705
	State Transition	705
	Configuring Clustering	706
	<i>Setting Interface Mode</i>	707
	<i>Management Access for ASDM Deployment</i>	708
	<i>Building a Cluster</i>	710
	<i>Data Interface Configuration</i>	714
	Monitoring and Troubleshooting Clustering	717
	Spanned EtherChannel Cluster Deployment Scenario	720
<b>Chapter 17</b>	<b>Implementing Cisco ASA Intrusion Prevention System (IPS)</b>	<b>733</b>
	IPS Integration Overview	733
	IPS Logical Architecture	735
	IPS Hardware Modules	735
	IPS Software Modules	736
	Inline and Promiscuous Modes	737
	IPS High Availability	739
	Cisco IPS Software Architecture	739
	MainApp	741
	<i>AuthenticationApp</i>	741
	<i>Attack Response Controller</i>	742
	<i>cipsWebserver</i>	742
	Logger	742
	<i>CtlTransSource</i>	743
	<i>NotificationApp</i>	743
	SensorApp	743
	CollaborationApp	744
	EventStore	744
	Preparing ASA IPS for Configuration	744
	Installing CIPS System Software	744
	Accessing CIPS from the ASA CLI	747
	Configuring Basic Management Settings	748
	Setting Up ASDM for IPS Management	752
	Installing the CIPS License Key	752
	Configuring CIPS Software on ASA IPS	753
	Custom Signatures	755

Remote Blocking	758
Anomaly Detection	763
Global Correlation	766
Maintaining ASA IPS	768
User Account Administration	769
<i>Administrator Account</i>	769
<i>Operator Account</i>	769
<i>Viewer Account</i>	769
<i>Service Account</i>	770
<i>Adding, Changing, and Deleting Users</i>	770
Displaying CIPS Software and Process Information	771
Upgrading CIPS Software and Signatures	772
<i>One-Time Upgrades</i>	773
<i>Scheduled Upgrades</i>	774
Backing Up ASA IPS Configuration	776
Displaying and Clearing Events	776
Configuring ASA for IPS Traffic Redirection	778
Botnet Traffic Filter	780
Dynamic and Local Blacklist Data	781
DNS Snooping	782
Traffic Selection	783
<b>Chapter 18 Tuning and Monitoring IPS</b>	<b>787</b>
IPS Tuning Process	787
Risk Ratings	789
ASR	790
TVR	790
SFR	790
ARR	791
PD	791
WLR	791
Disabling IPS Signatures	791
Retiring IPS Signatures	792
Tools to Help with Monitoring and Tuning	793
ASDM and IME	793
CSM Event Manager	794
Removing False Positive IPS Events from the Event Table	794
Splunk	794
RSA Security Analytics	794
Displaying and Clearing Statistics in the Cisco ASA IPS	795



**Chapter 19 Site-to-Site IPsec VPNs 801**

Preconfiguration Checklist	802
Configuration Steps	805
Step 1: Enable ISAKMP	806
Step 2: Create the ISAKMP Policy	807
Step 3: Set Up the Tunnel Groups	808
Step 4: Define the IPsec Policy	810
Step 5: Create a Crypto Map	812
Step 6: Configure Traffic Filtering (Optional)	816
Step 7: Bypass NAT (Optional)	817
Step 8: Enable Perfect Forward Secrecy (Optional)	819
Alternative Configuration Methods Through ASDM	820
<i>Defining Site-to-Site Tunnel Using the IPsec VPN Wizard</i>	820
<i>Defining a Site-to-Site Tunnel Through a Connection Profile</i>	821
Optional Attributes and Features	822
OSPF Updates over IPsec	823
Reverse Route Injection	824
NAT Traversal	826
Tunnel Default Gateway	827
Management Access	828
Fragmentation Policies	829
Deployment Scenarios	830
Single Site-to-Site Tunnel Configuration Using NAT-T, RRI, and IKEv2	831
<i>Configuration Steps Through ASDM</i>	831
<i>Configuration Steps Through CLI</i>	833
Hub and Spoke Using Security Contexts	836
<i>Configuration Steps Through ASDM</i>	837
<i>Configuration Steps Through CLI</i>	842
Monitoring and Troubleshooting Site-to-Site IPsec VPNs	848
Monitoring Site-to-Site VPNs	848
Troubleshooting Site-to-Site VPNs	852
<i>ISAKMP Proposal Unacceptable</i>	854
<i>Mismatched Preshared Keys</i>	854
<i>Incompatible IPsec Transform Set</i>	854
<i>Mismatched Proxy Identities</i>	855
<i>ISAKMP Captures</i>	856

**Chapter 20 IPsec Remote-Access VPNs 859**

Cisco IPsec Remote Access VPN Solution	860
IPsec (IKEv1) Remote-Access Configuration Steps	862
<i>Using the ASDM IPsec IKEv1 Remote Access VPN Wizard</i>	863

<i>Manually Configuring IPsec (IKEv1) VPN Using ASDM and CLI</i>	871
<i>Configuring Group Policies</i>	875
<i>Configuring a Tunnel Group</i>	876
IPsec (IKEv2) Remote-Access Configuration Steps	889
<i>Step 1: Introduction</i>	889
<i>Step 2: Connection Profile Identification</i>	890
<i>Step 3: VPN Protocols</i>	890
<i>Step 4: Client Images</i>	893
<i>Step 5: Specify User Authentication Method</i>	893
<i>Step 6: Specify an Address Pool</i>	893
<i>Step 7: Network Name Resolution Servers</i>	893
<i>Step 8: NAT Exemption</i>	894
<i>Step 9: AnyConnect Client Deployment</i>	894
Hardware-Based VPN Clients	894
Advanced Cisco IPsec VPN Features	896
Tunnel Default Gateway	896
Transparent Tunneling	897
NAT Traversal	898
IPsec over UDP	898
IPsec over TCP	899
IPsec Hairpinning	899
VPN Load Balancing	901
Client Firewalling	904
<i>Personal Firewall Check</i>	904
<i>Central Protection Policy</i>	906
Hardware-Based Easy VPN Client Features	907
<i>Interactive Client Authentication</i>	907
<i>Individual User Authentication</i>	908
<i>LEAP Bypass</i>	909
<i>Cisco IP Phone Bypass</i>	909
<i>Hardware Client Network Extension Mode</i>	909
L2TP over IPsec Remote-Access VPN (IKEv1)	910
L2TP over IPsec Remote-Access Configuration Steps	912
<i>Step 1: Select Tunnel Interface</i>	913
<i>Step 2: Select Remote Access Client</i>	914
<i>Step 3: Select VPN Client Authentication Method</i>	914
<i>Step 4: Specify User Authentication Method</i>	914
<i>Step 5: User Accounts</i>	914
<i>Step 6: Specify an Address Pool</i>	915
<i>Step 7: Specify Attributes Pushed to Clients</i>	915

<i>Step 8: Select the IPsec Settings (Optional)</i>	915
<i>Step 9: Verify the Configuration</i>	915
Windows L2TP over IPsec Client Configuration	915
Deployment Scenarios	916
Load Balancing of Cisco IPsec Clients and Site-to-Site Integration	916
<i>Configuration Steps Through ASDM</i>	917
<i>Configuration Steps Using the CLI</i>	919
Monitoring and Troubleshooting Cisco Remote-Access VPNs	922
Monitoring Cisco Remote-Access IPsec VPNs	922
Troubleshooting Cisco IPsec VPN Clients	926
<b>Chapter 21 Configuring and Troubleshooting PKI</b>	<b>931</b>
Introduction to PKI	931
Certificates	932
Certificate Authority	933
Certificate Revocation List	935
Simple Certificate Enrollment Protocol	936
Installing Certificates	936
Installing Certificates Through ASDM	936
<i>Installing a CA Certificate from a File</i>	937
Installing an Identity Certificate from a File	938
Installing a CA Certificate by the Copy-and-Paste Method	939
Installing a CA Certificate Using SCEP	940
Installing an Identity Certificate Using SCEP	943
Installing Certificates Using the CLI	945
<i>Generating the RSA Key Pair in the CLI</i>	945
<i>Configuring a Trustpoint</i>	946
<i>Manual (Cut-and-Paste) Enrollment via the CLI</i>	951
<i>Configuring CRL Options via the CLI</i>	954
The Local Certificate Authority	957
Configuring the Local CA Through ASDM	958
Configuring the Local CA Using the CLI	960
Enrolling Local CA Users Through ASDM	963
Enrolling Local CA Users Through the CLI	965
Configuring IPsec Site-to-Site Tunnels Using Certificates	966
Configuring the Cisco ASA to Accept Remote-Access IPsec VPN Clients Using Certificates	971
Troubleshooting PKI	972
Time and Date Mismatch	972
SCEP Enrollment Problems	975
CRL Retrieval Problems	977

**Chapter 22 Clientless Remote-Access SSL VPNs 979**

- SSL VPN Design Considerations 980
  - User Connectivity 981
  - ASA Feature Set 981
  - Infrastructure Planning 981
  - Implementation Scope 981
- SSL VPN Prerequisites 982
  - SSL VPN Licenses 983
    - AnyConnect Premium* 984
    - AnyConnect Essentials* 984
    - AnyConnect Mobile* 984
    - Shared Premium Licensing* 985
    - VPN Flex Licenses* 985
  - Client Operating System and Browser and Software Requirements 986
  - Infrastructure Requirements 987
- Pre-SSL VPN Configuration Guide 987
  - Enroll Digital Certificates (Recommended) 988
    - Step 1: Obtaining a CA Certificate* 988
    - Step 2: Request a Certificate* 989
    - Step 3: Apply Identity Certificate for SSL VPN Connections* 993
  - Set Up Tunnel and Group Policies 994
    - Configure Group Policies* 995
    - Configure a Tunnel Group* 998
  - Set Up User Authentication 1000
- Clientless SSL VPN Configuration Guide 1004
  - Enable Clientless SSL VPN on an Interface 1005
  - Configure SSL VPN Portal Customization 1006
    - Logon Page* 1007
    - Portal Page* 1012
    - Logout Page* 1015
  - Portal Customization and User Group* 1016
    - Full Customization* 1019
  - Configure Bookmarks 1024
    - Configure Websites* 1026
    - Configure File Servers* 1028
  - Apply a Bookmark List to a Group Policy* 1029
  - Single Sign-on* 1030
  - Configure Web-Type ACLs 1031
  - Configure Application Access 1034

<i>Configure Port Forwarding</i>	1035
<i>Configure Smart Tunnels</i>	1037
Configure Client-Server Plug-ins	1040
Cisco Secure Desktop	1041
CSD Components	1043
<i>Secure Desktop Manager</i>	1043
<i>Secure Desktop</i>	1043
<i>Cache Cleaner</i>	1043
CSD Requirements	1044
<i>Supported Operating Systems</i>	1044
<i>User Privileges</i>	1044
<i>Supported Internet Browsers</i>	1045
<i>Internet Browser Settings</i>	1045
CSD Architecture	1045
Configuring CSD	1046
<i>Step 1: Load the CSD Package</i>	1047
<i>Step 2: Define Prelogin Sequences</i>	1048
Host Scan	1054
Host Scan Modules	1054
<i>Basic Host Scan</i>	1055
<i>Endpoint Assessment</i>	1055
<i>Advanced Endpoint Assessment</i>	1055
Configuring Host Scan	1056
<i>Set Up Basic Host Scan</i>	1057
<i>Enable Endpoint Host Scan</i>	1058
<i>Set Up an Advanced Endpoint Host Scan</i>	1058
Dynamic Access Policies	1060
DAP Architecture	1061
DAP Sequence of Events	1062
Configuring DAP	1062
<i>Choose AAA Attributes</i>	1063
<i>Choose Endpoint Attributes</i>	1066
<i>Define Access Policies</i>	1068
Deployment Scenario	1075
Step 1: Define Clientless Connections	1076
Step 2: Configure DAP	1077
Monitoring and Troubleshooting SSL VPN	1078
Monitoring SSL VPN	1078
Troubleshooting SSL VPN	1081
<i>Troubleshooting SSL Negotiations</i>	1081

*Troubleshooting Clientless Issues* 1081

*Troubleshooting CSD* 1083

*Troubleshooting DAP* 1083

## **Chapter 23 Client-Based Remote-Access SSL VPNs 1085**

SSL VPN Deployment Considerations 1086

    Cisco AnyConnect Secure Mobility Client Licenses 1086

    Cisco ASA Design Considerations 1086

*ASA Feature Set* 1086

*Infrastructure Planning* 1086

*Implementation Scope* 1087

SSL VPN Prerequisites 1088

    Client Operating System and Browser and Software Requirements 1088

*Supported Operating Systems* 1088

*Compatible Browsers* 1089

    Infrastructure Requirements 1089

*ASA Placement and Requirements* 1089

*User Account* 1089

*Administrative Privileges* 1090

Pre-SSL VPN Configuration Guide 1090

    Enrolling Digital Certificates (Recommended) 1090

    Setting Up Tunnel and Group Policies 1090

*Configuring Group Policies* 1091

*Configuring a Tunnel Group* 1092

    Setting Up User Authentication 1094

Cisco AnyConnect Secure Mobility Client Configuration Guide 1096

    Loading the Cisco AnyConnect Secure Mobility Client Package 1096

    Defining the Cisco AnyConnect Secure Mobility Client Attributes 1098

*Enabling Cisco AnyConnect Secure Mobility Client VPN Client Functionality* 1099

*Defining a Pool of Addresses* 1101

    Advanced Full Tunnel Features 1103

*Split Tunneling* 1103

*DNS and WINS Assignment* 1106

*Keeping the SSL VPN Client Installed* 1107

*Configuring DTLS* 1108

*Configuring Traffic Filters* 1109

    AnyConnect Client Configuration 1109

*Creating AnyConnect Client Profile* 1110

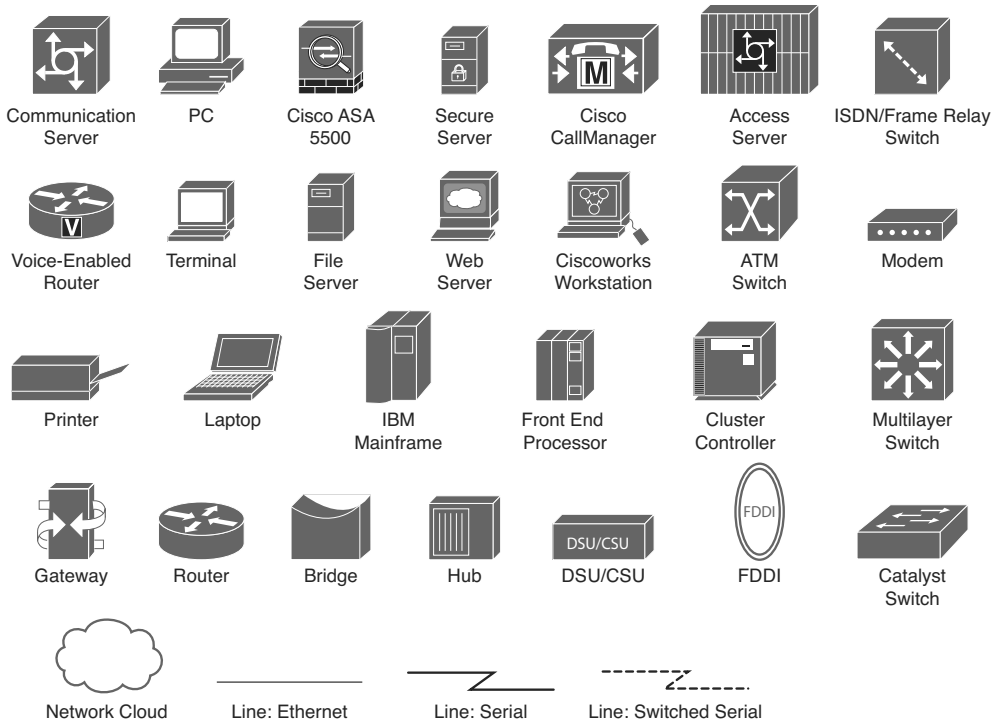
*Connecting from AnyConnect Client* 1112

Deployment Scenario of AnyConnect Client	1112
Step 1: Set Up CSD for Registry Check	1114
Step 2: Set Up RADIUS for Authentication	1114
Step 3: Configure AnyConnect SSL VPN	1115
Step 4: Enable Address Translation for Internet Access	1116
Monitoring and Troubleshooting AnyConnect SSL VPNs	1116
Troubleshooting SSL VPN	1116
<i>Troubleshooting SSL Negotiations</i>	1116
<i>Troubleshooting AnyConnect Client Issues</i>	1117
<b>Chapter 24 IP Multicast Routing</b>	<b>1119</b>
IGMP Support	1120
PIM Sparse Mode	1120
Configuring IP Multicast Routing	1120
Enabling Multicast Routing	1121
<i>Statically Assigning an IGMP Group</i>	1122
<i>Limiting IGMP States</i>	1122
<i>IGMP Query Timeout</i>	1123
<i>Defining the IGMP Version</i>	1123
Enabling PIM	1124
<i>Configuring Rendezvous Points</i>	1125
<i>Filtering PIM Neighbors</i>	1126
<i>Configuring a Static Multicast Route</i>	1127
Troubleshooting IP Multicast Routing	1127
Useful show Commands	1128
Useful debug Commands	1129
<b>Chapter 25 Quality of Service</b>	<b>1131</b>
QoS Types	1133
Traffic Prioritization	1133
Traffic Policing	1134
Traffic Shaping	1135
QoS Architecture	1136
Packet Flow Sequence	1136
Packet Classification	1137
<i>IP Precedence Field</i>	1137
<i>IP DSCP Field</i>	1138
<i>IP Access Control List</i>	1141
<i>IP Flow</i>	1141
<i>VPN Tunnel Group</i>	1141
QoS and VPN Tunnels	1142

Configuring Quality of Service	1142
QoS Configuration via ASDM	1143
<i>Step 1: Tune Priority Queue</i>	1143
<i>Step 2: Define a Service Policy</i>	1144
<i>Step 3: Specify Traffic Classification Criteria</i>	1145
<i>Step 4: Apply an Action Rule</i>	1148
QoS Configuration via CLI	1152
<i>Step 1: Tune the Priority Queue</i>	1152
<i>Step 2: Set Up a Class Map</i>	1152
<i>Step 3: Configure a Policy Map</i>	1153
<i>Step 4: Apply the Policy Map on the Interface</i>	1155
QoS Deployment Scenario	1155
Configuration Steps Through ASDM	1157
Configuration Steps Through the CLI	1160
Monitoring QoS	1162



## Icons Used in This Book



## Command Syntax Conventions

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

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

## Foreword

First, let me congratulate Jazib, Omar, and Andrew for producing what will be regarded as the definitive guide to maximizing the value of the Cisco Adaptive Security Appliance (ASA).

This book takes a hands-on approach to its subject and illuminates the design concepts and functionality built into the latest versions of the Cisco ASA, which allows technology organizations to secure data, services, and assets. The world has moved from IT infrastructure architectures consisting of enterprise-owned assets contained within a perimeter to a constantly changing mix of virtual, cloud, and outsourced environments. If anything, the enterprise IT security mission promises to become even more complex as the Internet of Things accelerates its expansion over the coming years.

So, if IT managers can no longer see, control, and secure the lion's share of assets for which they are responsible, what can they see, control, and secure? The network holds the answer to that question.

As the IT universe has evolved in ways beyond our imagining, the network itself has become the high ground for information security. Formerly, the only things that mattered in a network were bandwidth, availability, and cost of service. In a very real sense, the ideal network was an open, common carrier highway for all traffic—good, bad, and ugly.

Today, networks are much smarter than they used to be. They offer their operators unprecedented abilities to see, monitor, and control traffic traveling across them. The security benefits of smarter networks should go without saying at this point. The Cisco ASA leads this trend by integrating identity management, access control, intrusion prevention, and VPN services in a single system.

Technology alone, however, does not secure a network or an infrastructure. Infrastructure operators need to effectively use the tools available to them to minimize opportunities for adversaries to do harm. That's where this book comes in. It provides solid grounding in a proven strategy to get the most from the Cisco ASA.

In conclusion, knowledge is always more powerful than technology, and learning—as provided in this book—is the pathway to knowledge. This book will help you expand the efficacy of your ASA and help you gain some additional perspectives on network security.

Bryan Palma

Senior Vice President

Global Security Services

## Introduction

Cyber security has always been a challenge for many organizations, especially for those that cannot deploy separate devices to provide next-generation firewall, intrusion prevention, and virtual private network (VPN) services. The Cisco ASA is a high-performance, multifunction security appliance that offers next-generation firewall, IPS, and VPN services. The Cisco ASA delivers these features through improved network integration, resiliency, and scalability.

This book is an insider's guide to planning, implementing, configuring, and troubleshooting the Cisco Adaptive Security Appliances. It delivers expert guidance from senior Cisco security engineers. It demonstrates how adaptive identification and mitigation services on the Cisco ASA provide a sophisticated network security solution to small, medium, and large organizations. This book brings together expert guidance for virtually every challenge you will face—from building basic network security policies to advanced next-generation firewall, VPN, and IPS implementations.

## Who Should Read This Book?

This book serves as a guide for any network professional who manages network security or installs and configures firewalls, VPN devices, or intrusion detection/prevention systems. It encompasses topics from an introductory level to advanced topics on security and VPNs. The requirements of the reader include a basic knowledge of TCP/IP and networking.

## How This Book Is Organized

This book has four parts, which provide a Cisco ASA product introduction and then focus on firewall features, intrusion prevention, and VPNs. Each part includes many sample configurations, accompanied by in-depth analyses of design scenarios. Your learning is further enhanced by a discussion of a set of debugs included in each technology. Groundbreaking features, such as next-generation firewalls, clustering, virtual firewalls, and SSL VPN, are discussed extensively.

The following is an overview of how this book is organized:

Part I, “Product Overview,” includes the following chapters:

- Chapter 1, “Introduction to Security Technologies”: This chapter provides an overview of different technologies that are supported by the Cisco ASA and widely used by today's network security professionals.
- Chapter 2, “Cisco ASA Product and Solution Overview”: This chapter describes how the Cisco ASA incorporates features from each of these products, integrating comprehensive firewall, intrusion detection and prevention, and VPN technologies in a cost-effective, single-box format. Additionally, it provides a hardware overview of the Cisco ASA, including detailed technical specifications and installation guidelines. It also covers an overview of all the modules available for the Cisco ASA.

- Chapter 3, “Licensing”: Different features in the Cisco ASA require a license. This chapter describes the available licenses for each Cisco ASA model and specific features, and explains how to install such licenses. It also covers the details about how you can configure a Cisco ASA as a licensing server to share SSL VPN licenses among a group of Cisco ASA.
- Chapter 4, “Initial Setup”: A comprehensive list of initial setup tasks is included in this chapter. These tasks and procedures are intended to help network professionals to install, configure, and manage the basic features of the Cisco ASA.
- Chapter 5, “System Maintenance”: This chapter contains information about how to perform system maintenance of the Cisco ASA, including system upgrades and health monitoring, and provides tips to troubleshoot hardware and data issues.
- Chapter 6, “Cisco ASA Services Module”: The Cisco Catalyst 6500 Series and 7600 Series ASA Services Module (ASASM) is a scalable, high-performance blade that integrates with the Cisco Catalyst 6500 Series Switches and Cisco 7600 Series routers. It helps security administrators reduce costs and operational complexity, while allowing them to manage multiple firewalls from the same scalable switch platform. This chapter covers how to configure the Cisco ASA Services Module, as well as how to configure the Cisco Catalyst 6500 Series Switches and 7600 Series Routers to send traffic to be protected and inspected by the module.

Part II, “Firewall Technology,” includes the following chapters:

- Chapter 7, “Authentication, Authorization, and Accounting (AAA) Services”: The Cisco ASA supports a wide range of AAA features. This chapter provides guidelines on how to configure AAA services by defining a list of authentication methods applied to various implementations.
- Chapter 8, “Controlling Network Access: The Traditional Way”: The Cisco ASA can protect one or more networks from intruders. Connections between these networks can be carefully controlled by advanced firewall capabilities, enabling you to ensure that all traffic from and to the protected networks passes only through the firewall based on the organization’s security policy. This chapter shows you how to implement your organization’s security policy, using the features the Cisco ASA provides.
- Chapter 9, “Implementing Next-Generation Firewall Services with ASA CX”: Cisco ASA Next-Generation Firewall Services provides advanced security services including Application Visibility and Control (AVC) and Web Security Essentials (WSE). These new features provide granular application control that recognizes thousands of applications and provides context-based awareness of those applications and their users. This chapter covers the features, benefits, deployment, configuration, and troubleshooting of the Cisco ASA Next-Generation Firewall Services.

- Chapter 10, “Network Address Translation”: This chapter provides details on how to configure Network Address Translation (NAT) on the Cisco ASA. It covers the different address translation types, how to configure address translation, DNS doctoring, and monitoring address translations in the Cisco ASA. NAT configuration commands and underlying infrastructure changed in Cisco ASA Software version 8.3. This chapter includes both pre-8.3 and post-8.3 configuration commands and steps.
- Chapter 11, “IPv6 Support”: The Cisco ASA supports IPv6. This chapter covers the configuration and deployment of IPv6 support in the Cisco ASA.
- Chapter 12, “IP Routing”: This chapter covers the different routing capabilities of the Cisco ASA.
- Chapter 13, “Application Inspection”: The Cisco ASA stateful application inspection helps secure the use of applications and services in your network. This chapter describes how to use and configure application inspection.
- Chapter 14, “Virtualization”: The Cisco ASA virtual firewall feature introduces the concept of operating multiple instances of firewalls (contexts) within the same hardware platform. This chapter shows how to configure and troubleshoot each of these security contexts.
- Chapter 15, “Transparent Firewalls”: This chapter introduces the transparent (Layer 2) firewall model within the Cisco ASA. It explains how users can configure the Cisco ASA in transparent single mode and multiple mode while accommodating their security needs such as traffic filtering and address translation.
- Chapter 16, “High Availability”: This chapter discusses the different redundancy and high availability mechanisms that the Cisco ASA provides. It covers the configuration of advanced high scalability features such as clustering. The Cisco ASA clustering feature is used to combine up to sixteen supported appliances into a single traffic processing system. Unlike in failover, each unit of an ASA cluster actively forwards transit traffic in both single and multiple-context modes. This chapter includes not only the overview and configuration, but also detailed troubleshooting procedures of all the high availability features available in the Cisco ASA.

Part III, “Intrusion Prevention System (IPS) Solutions,” includes the following chapters:

- Chapter 17, “Implementing ASA Intrusion Prevention System (IPS)”: Intrusion detection and prevention systems provide a level of protection beyond the firewall by securing the network against internal and external attacks and threats. This chapter describes the integration of IPS features within the Cisco ASA and provides expert guidance on how to configure the Cisco IPS software. Troubleshooting scenarios are also included to enhance learning.
- Chapter 18, “Tuning and Monitoring IPS”: This chapter covers the IPS tuning process, as well as best practices on how to monitor IPS events.

Part IV, “Virtual Private Network (VPN) Solutions,” includes the following chapters:

- Chapter 19, “Site-to-Site IPsec VPNs”: The Cisco ASA supports IPsec VPN features that enable you to connect networks in different geographic locations. This chapter provides configuration and troubleshooting guidelines to successfully deploy site-to-site IPsec VPNs in both single- and multiple-mode firewalls.
- Chapter 20, “IPsec Remote-Access VPNs”: This chapter discusses two IPsec remote-access VPN solutions (Cisco IPsec and L2TP over IPsec) that are supported on the Cisco ASA. Numerous sample configurations and troubleshooting scenarios are provided.
- Chapter 21, “Configuring and Troubleshooting PKI”: This chapter begins by introducing Public Key Infrastructure (PKI) concepts. It then covers the configuration and troubleshooting of PKI in the Cisco ASA.
- Chapter 22, “Clientless Remote-Access SSL VPNs”: This chapter provides details about the clientless SSL VPN functionality in Cisco ASA. It covers the Cisco Secure Desktop (CSD) solution and also discusses the Host Scan feature that is used to collect posture information about an endpoint. The dynamic access policy (DAP) feature, its usage, and detailed configuration examples are also provided. To reinforce learning, many different deployment scenarios are presented along with their configurations.
- Chapter 23, “Client-Based Remote-Access SSL VPNs”: This chapter provides details about the AnyConnect SSL VPN functionality in Cisco ASA.
- Chapter 24, “IP Multicast Routing”: This chapter covers the configuration and troubleshooting of multicast routing support in the Cisco ASA.
- Chapter 25, “Quality of Service”: QoS is a network feature that allows you to give priority to certain types of traffic. This chapter covers how to configure, troubleshoot, and deploy the QoS features in the Cisco ASA.

*This page intentionally left blank*

*This page intentionally left blank*



## Licensing

This chapter covers the following topics:

- Licensed features on ASA
- Managing licenses with activation keys
- Combined licenses in failover and clustering
- Shared Premium AnyConnect VPN licensing

ASA offers a very comprehensive feature set that helps secure networks of all shapes and sizes. To deliver the desired functionality within the available budget while allowing for future scalability, you can unlock advanced security capabilities and increase certain system capacities on demand through a flexible system of feature licenses.

Some characteristics of the hardware platform or expansion modules can enable certain feature licenses implicitly. You can also activate additional licenses permanently or for a certain duration of time. When multiple Cisco ASA devices participate in failover or clustering, some licensed capacities automatically aggregate up to the platform hardware limit to maximize your investment. Although this flexible system may seem complicated at first, it actually makes the task of customizing a Cisco ASA for your specific business needs quite easy.

### Licensed Features on ASA

Every Cisco ASA platform comes with a certain number of implicitly activated features and capacities as a part of the Base License. In other words, these capabilities are fixed in the given software image for the particular hardware; you cannot selectively disable them. One example of such a feature is Active/Active failover, which is always available on all Cisco ASA 5585-X appliances. Some platforms offer the optional Security Plus license, which may unlock additional features or capacities on top of the Base License.

For example, you can increase the maximum concurrent firewall connection count on the Cisco ASA 5505 from 10,000 to 25,000 by installing a Security Plus license.

In addition to the Base and Security Plus licenses, you can activate other advanced security features individually:

- Some capabilities operate in a simple binary switch fashion whereby the license for the feature type is either enabled or disabled; once enabled, there are typically no direct restrictions on how much the feature can be used. For instance, the Botnet Traffic Filter license will allow you to protect all connections through a Cisco ASA up to the maximum limit for the platform.
- Other features may carry their own capacity limits that come in quantified tiers. An example of such a feature is the ability to configure security contexts on some Cisco ASA appliances. On the Cisco ASA 5580 platform, the Base License allows creating up to two application contexts, while several premium licenses of different tiered counts allow extending this limit up to 250 contexts in total.

Not all of the licensed features and capabilities are available on all hardware platforms. For instance, at the time of writing, the clustering feature is currently available only on Cisco ASA 5500-X, ASA 5580, and ASA 5585-X appliances. Depending on specific markets and international export regulations, some Cisco ASA models may also ship with the permanent No Payload Encryption license; this license ties to the particular hardware without the option of change or removal. The following licensed features and capacities are not available on any No Payload Encryption hardware models:

- AnyConnect Premium Peers
- AnyConnect Essentials
- Other VPN Peers
- Total VPN Peers
- Shared License
- AnyConnect for Mobile
- AnyConnect for Cisco VPN Phone
- Advanced Endpoint Assessment
- UC Phone Proxy Sessions
- Total UC Proxy Sessions
- Intercompany Media Engine

As you identify the correct feature set to take the most advantage of Cisco ASA capabilities while fully protecting your network, it helps to organize the licensed features into the following logical categories:

- **Basic platform capabilities:** Typically are relevant to all Cisco ASA deployments
- **Advanced security features:** Can satisfy specific network design goals for a particular Cisco ASA installation
- **Tiered capacity features:** Depend on the size of a projected user base and allow for future growth

These categories are discussed in turn next.

## Basic Platform Capabilities

Basic licensed features define the foundation of the Cisco ASA capabilities that are common to all installations and designs, such as the following:

- Dictating the elementary characteristics of how an ASA device connects to the network
- Establishing the quantity and speed capabilities of physical and logical interfaces
- Limiting the number of protected connections and inside hosts
- Defining high-availability options
- Setting the baseline encryption algorithms that the system can use

The following licensed features fall under the category of basic platform capabilities:

- **Firewall Connections:** Cisco ASA Software limits the maximum concurrent count of all stateful connections depending on the hardware platform. This limit can only be increased with the Security Plus license on Cisco ASA 5505, ASA 5510, and ASA 5512-X appliances. The system will deny only new attempted connections above the licensed limit; there are no adverse effects for existing connections in this case.
- **Maximum Physical Interfaces:** All Cisco ASA platforms always allow you to use all of the available physical interfaces, so this feature either shows the actual number of physical interfaces on the Cisco ASA 5505 or displays Unlimited on all other platforms. There are additional platform-specific limitations on the total number of interfaces that can be configured in the system; the total limit covers physical and redundant interfaces, VLAN subinterfaces, EtherChannels, and bridge groups.
- **Maximum VLANs:** Each platform has its own limit on the maximum number of configurable VLANs. This limit can be expanded on Cisco ASA 5505, ASA 5510, and ASA 5512-X models by applying a Security Plus license. Keep in mind that you can create a larger number of subinterfaces on some ASA appliances, but this particular limit only kicks in when you actually assign the given number of subinterfaces to VLANs with the `vlan` interface command.

- **VLAN Trunk Ports:** This feature is applicable only to Cisco ASA 5505 appliances because they have the built-in Ethernet switch. With the Base License, you can configure the physical switch ports only in access mode; with the Security Plus license, you gain the ability to carry multiple VLANs on any of the Cisco ASA 5505 physical interfaces by configuring them as trunks.
- **Dual ISPs:** This feature only applies to the Cisco ASA 5505 where the Security Plus license enables it automatically. With the Base License, this platform only allows up to three configured logical interfaces, where the third interface can initiate traffic only to one of the other two; with this limitation, you cannot create a backup interface to provide external connectivity when the primary outside interface fails. When you apply the Security Plus license, the number of available logical interfaces increases to 20; you can then use floating default routes with route tracking to enable interface-level high availability across multiple ISPs.
- **10GE I/O:** This feature is only applicable to Cisco ASA 5585-X models. An SSP-10 and -20 with the Base License only allow you to configure the onboard fiber interfaces at 1-Gigabit Ethernet (GE) speed; the Security Plus license enables configuring these interfaces at 10-GE speed. This capability is always enabled on SSP-40 and -60 and on any expansion 10-GE interface modules. Although not directly related to this license, it should be noted that a Cisco ASA 5510 appliance requires the Security Plus license to configure Ethernet0/0 and Ethernet0/1 interfaces at 1-GE speed. All other models not mentioned here allow you to configure any onboard or external physical Ethernet interfaces up to the maximum supported speed.
- **Inside Hosts:** This value defines the maximum number of unique IP addresses behind the trusted interfaces that can establish concurrent connections with endpoints behind the outside interface. When operating in routed mode, the default route determines where the outside interface is; all unique endpoints behind all configured interfaces count toward the limit if the default route is not present. In transparent mode, only the interface with the fewest number of active endpoints counts toward the limit. This feature is set to Unlimited on all platforms except the Cisco ASA 5505, whose default limit of 10 can be expanded to 50 or Unlimited.
- **Failover:** The option of configuring a pair of Cisco ASA devices for high availability is available on all platforms, but it requires the Security Plus license on Cisco ASA 5505, ASA 5510, and ASA 5512-X models. Because the Cisco ASA 5505 does not support the Security Contexts feature, only Active/Standby failover is available on this platform. All other ASA models support both Active/Standby and Active/Active failover configurations.
- **Encryption-DES:** This license enables the DES algorithm for VPN, Unified Communications Proxy, and management session encryption by default on all Cisco ASA platforms. A weak encryption algorithm such as DES is frequently not acceptable to many remote endpoints that need to establish a secure session with the Cisco ASA; this license is typically not sufficient outside of basic management tasks.

- **Encryption-3DES-AES:** This license adds 3DES and AES algorithms in order to provide strong encryption capabilities for VPN, Unified Communications Proxy, and management sessions. Some features, such as VPN Load Balancing, also require this license for proper operation. Export regulations control access to this license, so it may not necessarily come pre-installed on a brand-new Cisco ASA by default. Because the availability of strong encryption ciphers in the Cisco ASA configuration requires this license, obtain and enable it right away if you plan on using any of the relevant cryptographic features.
- **Other VPN Peers:** This value defines the maximum number of concurrent IPsec site-to-site tunnels and IKEv1-based remote-access sessions that can terminate on a particular Cisco ASA platform. This capacity can extend from 10 to 25 by installing the Security Plus license on the Cisco ASA 5505; on all of the other models, the software sets this limit depending on the hardware capabilities.
- **Total VPN Peers:** This quantity defines the maximum number of any concurrent VPN sessions that can terminate on a given Cisco ASA platform. This licensed capacity is equal to the count of Other VPN Peers on all models with the exception of the Cisco ASA 5505, where it depends on the Security Plus and AnyConnect Essentials licenses.

## Advanced Security Features

You can leverage advanced security features on top of the core Cisco ASA capabilities to achieve an additional level of protection or to enable more complex network designs. These features include the following capabilities:

- Applying the delivery of specialized application protocol inspection
- Extending the secure network perimeter by supporting mobile platforms
- Performing client posture validation for VPN connectivity
- Enabling real-time mitigation of malicious activity
- Delivering scalable device aggregation capabilities

The following licensed features fall into this category:

- **Intercompany Media Engine:** With this feature enabled, a Cisco ASA becomes an active participant in the Intercompany Media Engine infrastructure, where the Session Initiation Protocol (SIP) inspection engine operates with TLS proxy to authenticate and secure dynamic incoming VoIP connections. Because there is a particular platform limit on the maximum number of TLS proxy sessions, Intercompany Media Engine shares this limit with other features that rely on TLS proxy. Depending on the export restrictions, the particular license for this feature may allow either a total of 1000 TLS proxy sessions (restricted) or up to the preset

platform limit (unrestricted). After applying this license, use the **tls-proxy maximum-sessions** command to raise the configured session limit as desired. It should be noted that other Unified Communications inspection features that rely on TLS proxy may impose separate limits on the total number of encrypted sessions.

- **GTP/GPRS:** This enables the application inspection of the GPRS Tunneling Protocol (GTP), which supports general packet radio service (GPRS) data networks. Mobile service providers commonly use this feature to secure their network infrastructure. After activating the license, use the **inspect gtp** command to enable the GTP/GPRS inspection engine on applicable traffic under the service policy configuration.
- **AnyConnect for Mobile:** This license allows a Cisco ASA to accept SSL VPN connections from certain mobile devices running Apple iOS, Android, and Windows Mobile operating systems. Keep in mind that this is not a standalone feature but rather a special capability available for AnyConnect peers. As such, you can utilize this capability only when an installed AnyConnect Premium Peers or AnyConnect Essentials license allows the underlying SSL VPN session. When the session is using an AnyConnect Essentials license, mobile device posture data is only available for informational purposes. When the mobile device is one of the AnyConnect Premium Peers, you can leverage Dynamic Access Policies (DAP) to permit or deny network access for the given device based on a broad set of attributes.
- **AnyConnect for Cisco VPN Phone:** This license allows a Cisco ASA to accept VPN connections from certain hardware Cisco IP phones that provide embedded AnyConnect client capabilities. This is not a standalone feature, because it requires an AnyConnect Premium Peers license to allow the underlying VPN connection in the first place.
- **Advanced Endpoint Assessment:** With this feature enabled, ASA can actively enforce certain operational policies on third-party antivirus, antispyware, and personal firewall software packages residing on remote AnyConnect or clientless peers running Microsoft Windows, Apple OS X, and Linux operating systems. This is another add-on feature that is only available for AnyConnect Premium Peers; by default, such peers can only benefit from the basic reactive posture validation capabilities provided by Host Scan and Dynamic Access Policies.
- **Botnet Traffic Filter:** With this feature, you can detect and block inbound and outbound connections that involve known malicious hosts. A Cisco ASA dynamically updates the database of such offending endpoints from Cisco Security Intelligence Operations (SIO), which allows real-time protection even for zero-day attacks. The license enables database updates as well as the Botnet Traffic Filter configuration commands.
- **Cluster:** This feature is currently available only on Cisco ASA 5500-X, ASA 5580, and ASA 5585-X appliances. It expands the high-availability advantages of failover by allowing you to aggregate up to 16 physical appliances in exactly the same hardware configuration into a single logical device. Unlike failover, all members of a configured cluster process transit traffic concurrently while compensating for

the imperfections of external load-balancing. All devices in a cluster must have this feature enabled. The availability of the Cluster feature and the maximum supported number of cluster members depend on the particular software image version and hardware platform type.

- **IPS Module:** This feature is only applicable to Cisco ASA 5500-X appliances. It allows you to implement Cisco ASA Intrusion Prevention System (IPS) with the software package; you do not need it for Cisco ASA Next-Generation Firewall Services with the CX package. This license simply allows you to install the IPS software module on the Cisco ASA and then enable traffic redirection using the service-policy configuration; because the module runs an independent software image, it has its own feature license that you have to obtain and install separately. Hardware IPS modules on Cisco ASA 5505, ASA 5500, and ASA 5585-X appliances require no special license for installation or traffic redirection.

## Tiered Capacity Features

Yet another category of licensed features allows a particular advanced functionality for a limited number of users or sessions. This flexibility allows you to provision enough premium licenses according to the specific business needs while allowing plenty of room for future growth. The typical features in this category provide firewall virtualization capabilities, Unified Communications inspection with TLS proxy, and advanced VPN connectivity. The preinstalled Base Licenses typically include a certain number of allowed sessions to take advantage of most of these features; you can obtain a separate license to enable or upgrade any of these capabilities to your desired user or session count. To keep things simple, these features come in specific capacity tiers. For instance, a Cisco ASA 5512-X with the Base License allows up to two Unified Communications (UC) Phone Proxy sessions; you can optionally obtain a license for 24, 50, 100, 250, or 500 sessions. Keep in mind that the capacity tiers cannot be stacked together. In other words, you need to obtain the UC Phone Proxy license for 250 sessions even if you intend to use only up to 150 of them; you cannot simply install a 50-session license followed by a 100-session license on the same device.

The following features belong to this category:

- **Security Contexts:** This license allows the creation of multiple virtual firewalls that can operate concurrently on the same physical ASA device. It is not available on the Cisco ASA 5505 platform or Cisco ASA 5510 and ASA 5512-X appliances with the Base License. All other platforms and license combinations allow you to configure up to two virtual application contexts by default; the specific tiered options depend on the platform and can extend up to 250 on a Cisco ASA Services Module and ASA 5585-X appliances with at least an SSP-20. Keep in mind that not all features are currently compatible with the multiple context mode even if you install the appropriate feature license.
- **UC Phone Proxy Sessions:** This value determines the maximum number of TLS proxy sessions that the UC Phone Proxy feature can use. This limit does not cover

transit VoIP connections that rely on the cleartext application inspection. Keep in mind that the number of active TLS proxy sessions may exceed the number of active VoIP endpoints, depending on their high-availability configuration. Typically, this licensed session count is equivalent to the Total UC Proxy Sessions license, which has the default value of 2 on all platforms. The Cisco ASA Services Module and ASA 5585-X appliances with at least an SSP-20 limit the maximum capacity of this feature to 5000 even with the Total UC Proxy Session license for 10,000 sessions. Refer to the description of the Intercompany Media Engine license for information about raising the default configured limit of TLS proxy sessions and determining additional session limits imposed by the export restrictions.

- **Total UC Proxy Sessions:** Similarly to UC Phone Proxy Sessions, this license establishes the maximum number of all connections that use TLS proxy to support Phone Proxy, Presence Federation Proxy, and Encrypted Voice Inspection features; this limit does not include TLS proxy sessions that relate to the Intercompany Media Engine or Mobility Advantage Proxy features. The default licensed capacity of this feature is 2 on all platforms; it can extend up to 10,000 sessions on a Cisco ASA Services Module or ASA 5585-X appliances with at least an SSP-20. Refer to the description of the Intercompany Media Engine license for information about raising the default configured limit of TLS proxy sessions and determining additional session limits imposed by export restrictions.
- **AnyConnect Premium Peers:** This value defines the maximum number of concurrent SSL VPN, Clientless SSL VPN, and IPsec IKEv1-based remote-access VPN sessions that can terminate on a particular Cisco ASA platform. This license is a prerequisite for multiple premium features that an AnyConnect Essentials license does not support. Such premium licensed features include AnyConnect for Cisco VPN Phone and Advanced Endpoint Assessment; Cisco Secure Desktop is another example. Keep in mind that the AnyConnect Premium Peers and AnyConnect Essential licenses cannot operate concurrently; even if you install both licenses on a single Cisco ASA device, only one of them stays active at any given time. You must use the `no anyconnect-essentials` command to enable the AnyConnect Premium Peers license. Although this tiered limit is separate from Other VPN Peers, the total concurrent VPN session count cannot exceed the Total VPN Peers.
- **AnyConnect Essentials:** This license allows the given number of SSL VPN and IPsec IKEv1-based remote-access VPN sessions to terminate on a particular Cisco ASA platform; it does not provide the ability to terminate Clientless SSL VPN connections. Refer to the description of the AnyConnect Premium Peers license for additional information on specific differences, concurrency implications, and overall limits that pertain to these related feature licenses.

## Displaying License Information

Use the `show version` or `show activation-key` command to display the complete list of licensed features and capacities of a particular Cisco ASA device along with the activation information. Example 3-1 shows sample output of the `show activation-key`



command issued on a Cisco ASA 5525-X appliance. Notice that the count of Firewall Connections does not show up as a licensed feature; check the output of the **show resource usage** command for some of these platform capacities. However, this sample output contains several pieces of additional information: the serial number of the appliance and the remaining active time for each feature. It also lists multiple activation keys that enable the given set of features on this particular device for the specified amount of time. These activation keys enable a straightforward mechanism for adding or removing licensed features on Cisco ASA devices.

### Example 3-1 Cisco ASA License Information

```
ciscoasa# show activation-key
Serial Number: FCH16447Q8L
Running Permanent Activation Key: 0x380df35d 0xe451697e 0xcd509dd4 0xeea888f4
0x001bc79c
Running Timebased Activation Key: 0x493c3ecd 0xcd6458a1 0x31b5a533 0xc970a48b
0x05867295
```

Licensed features for this platform:

Maximum Physical Interfaces	: Unlimited	perpetual
Maximum VLANs	: 200	perpetual
Inside Hosts	: Unlimited	perpetual
Failover	: Active/Active	perpetual
Encryption-DES	: Enabled	perpetual
Encryption-3DES-AES	: Enabled	56 days
Security Contexts	: 2	perpetual
GTP/GPRS	: Disabled	perpetual
AnyConnect Premium Peers	: 2	perpetual
AnyConnect Essentials	: Disabled	perpetual
Other VPN Peers	: 750	perpetual
Total VPN Peers	: 750	perpetual
Shared License	: Disabled	perpetual
AnyConnect for Mobile	: Disabled	perpetual
AnyConnect for Cisco VPN Phone	: Disabled	perpetual
Advanced Endpoint Assessment	: Enabled	56 days
UC Phone Proxy Sessions	: 2	perpetual
Total UC Proxy Sessions	: 2	perpetual
Botnet Traffic Filter	: Enabled	56 days
Intercompany Media Engine	: Disabled	perpetual
IPS Module	: Disabled	perpetual
Cluster	: Disabled	perpetual

This platform has an ASA5525 VPN Premium license.

The flash permanent activation key is the SAME as the running permanent key.

```

Active Timebased Activation Key:
0x493c3ecd 0xcd6458a1 0x31b5a533 0xc970a48b 0x05867295
Encryption-3DES-AES           : Enabled    56 days
Advanced Endpoint Assessment   : Enabled    56 days
Botnet Traffic Filter          : Enabled    56 days

```

## Managing Licenses with Activation Keys

An activation key is an encoded bit string that defines the list of features to enable, how long the key would stay valid upon activation, and the specific serial number of a Cisco ASA device. A series of five hexadecimal numbers, as shown at the top of the output in Example 3-1, typically represents that string. Each activation key is only valid for the particular hardware platform with the specific encoded serial number. The complete set of activation keys resides in a hidden partition of the built-in flash device of a Cisco ASA; other nonvolatile internal memory structures maintain a backup copy of that information. After Cisco generates a key for a given device, you cannot separate individual features from this licensed package. You can request and apply another key with a different set of features to the same Cisco ASA device at any future point in time. All features encoded in a particular key always have the same licensed duration, so activation keys can be classified as permanent or time-based.

### Permanent and Time-Based Activation Keys

Every Cisco ASA model comes with a certain set of basic features and capacities enabled by default; the Base License permanently activates these features on the particular platform. Even though these core features do not require an explicit activation key, one usually comes installed anyway. This is the permanent activation key, which never expires. Although the system does not require this key for basic operation, some advanced features, such as failover, depend on the permanent activation key in order to operate correctly. You can enable additional features without a time limit by applying a different permanent activation key. Because a Cisco ASA device can have only one permanent activation key installed at any given time, every new key must encompass the entire set of desired features. The feature set enabled by the new permanent activation key completely replaces the previously enabled permanent feature set, instead of merging with it. In rare situations in which the permanent activation key becomes lost or corrupted, the output of the **show activation-key** command displays the following value:

```

Running Permanent Activation Key: 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000

```

If this happens, the system continues to operate with the default set of basic features for the platform. Reinstall the permanent activation key to restore the desired feature set. Although you can always obtain the replacement key from Cisco, it is a best practice to always maintain a backup of all activation keys used by your Cisco ASA devices.

In addition to the permanent activation key, you can install one or more time-based keys to enable certain features for a limited period of time. All premium features can be activated by either permanent or time-based keys, with the exception of Botnet Traffic Filter, which is only available via a time-based license. Even though you can apply multiple time-based activation keys on the same Cisco ASA concurrently, only one license remains active for any particular feature at any given time. Thus, several time-based keys can stay active on the ASA as long as they enable different features. Other time-based keys remain installed but inactive until needed. Only the currently active licenses for each feature continue the time countdown; you can stop the timer by manually deactivating a key or installing a different time-based license for the same feature. In Cisco ASA Software version 8.3(1) and later, time-based key expiration no longer depends on the configured system time and date; the countdown occurs automatically based on the actual uptime of the ASA.

## Combining Keys

Even though only one time-based activation key can be active for any particular feature at any given time, two identical time-based keys will license a feature for the combined duration. All of the following conditions must be satisfied for this to happen:

- Both current and new time-based keys enable only one feature. Typically, this is how you receive all time-based activation keys from Cisco.
- Both keys license the feature at exactly the same level. If the feature is tiered, the licensed capacities have to match.

For example, assume that you have a Cisco ASA 5555-X with an active time-based key that enables 1000 AnyConnect Premium Peers for six weeks. If you add another time-based key for 1000 AnyConnect Premium Peers that has a duration of eight weeks, the new key will have the combined duration of 14 weeks. However, the new key will deactivate the original time-based license if it enables 2500 AnyConnect Premium Peers instead or also adds the Intercompany Media Engine feature. If you install another time-based key for the IPS Module feature on the same device, both keys will activate concurrently because they enable different features. To ease the management of time-based licenses and receive the maximum advantage of combining their duration when possible, always make sure to use separate time-based activation keys for each feature and tiered capacity.

When activated on the same device, the features and capacities of the permanent and active time-based keys also combine to form a single feature set, as such:

- The system chooses the better value between the two key types for any feature that can be either enabled or disabled. For example, the ASA enables the Intercompany Media Engine feature based on the permanent key even if all active time-based keys have this feature disabled.
- For AnyConnect Premium Sessions and AnyConnect Essentials licenses that are tiered, the system picks the highest session count between the active time-based and permanent keys.

- Total UC Proxy and Security Contexts counts combine between the permanent and active time-based keys up to the platform limit. This way, you can configure a total of 22 virtual contexts by adding a time-based license for 20 contexts to a Cisco ASA 5515-X with the permanent Base License for 2 contexts.

Example 3-1 illustrates a Cisco ASA that derives its feature set from the permanent and one time-based activation keys. Both activation keys appear at the top of the output. Features denoted as *perpetual* come from the permanent activation key; these licenses never expire. Time-based features show the remaining number of days before expiration; even if you enable one of these features via the permanent key later on, the countdown will continue until the applicable time-based key expires or becomes deactivated manually.

### Time-Based Key Expiration

When a time-base key is within 30 days of expiration, ASA generates daily system log messages to alert you of that fact. The following message includes the specific time-based activation key that is about to expire:

```
%ASA-4-444005: Timebased license key 0x8c9911ff 0x715d6ce9 0x590258cb
0xc74c922b 0x17fc9a will expire in 29 days.
```

When the active time-based license expires, a Cisco ASA looks for another available time-based activation key that you previously installed. The system picks the next key according to internal software rules, so a particular order is not guaranteed. You can manually activate a specific time-based key at any given time; after you do so, the deactivated time-based key remains installed with the unused licensed time still available. When all time-based keys for a particular feature expire, the device falls back to using the value in the permanent key for this feature. Upon any expiration event, an ASA generates another system log message that lists the expired key and the succession path for the license. The following message shows that the states of all licensed features from the expired time-based key reverted to the permanent key:

```
%ASA-2-444004: Timebased activation key 0x8c9911ff 0x715d6ce9 0x590258cb
0xc74c922b 0x17fc9a has expired. Applying permanent activation key 0x725e3a19
0xe451697e 0xcd509dd4 0xeea888f4 0x1bc79c.
```

As time-based licenses expire, certain features may deactivate completely and some licensed capacities of other features may reduce. Although these changes typically do not affect existing connections that are using a previously licensed feature, new connections will see the impact. For instance, assume that a Cisco ASA 5545-X appliance has the permanent activation key for 100 AnyConnect Premium Peers and a time-based license for 1000 AnyConnect Premium Peers. If there are 250 active clientless SSL VPN peers connected when the time-based key expires, the ASA appliance will not admit any new SSL VPN users until the session count drops below 100. However, the existing user sessions would remain operational with no impact. On the other hand, the Botnet Traffic Filter feature disables dynamic updates when the license expires; this removes the benefits of the feature right away.

Some features may show no impact from the time-based key expiration until the Cisco ASA system reloads; because the feature is no longer licensed upon the reload, the device may reject some elements of the startup configuration. When a Cisco ASA that was previously licensed for 20 security contexts reloads with the default license, only two virtual contexts will remain operational after the system loads the startup configuration file. To avoid unexpected network outages, it is very important to monitor time-based licenses for expiration and replace them in advance; always use permanent licenses for the critical features when possible.

## Using Activation Keys

To apply an activation key to the Cisco ASA, you can use the **activation-key** command followed by the hexadecimal key value. Both permanent and time-based keys follow the same process, and you cannot determine the key duration until you attempt to install it. Example 3-2 shows a successful attempt to activate the permanent key. Keep in mind that an ASA supports only one of such keys at any given time; the feature set of the last installed key completely overwrites the previous one.

### Example 3-2 *Successfully Activated Permanent Key*

```
ciscoasa# activation-key 813cd670 704cde05 810195c8 e7f0d8d0 4e23f1af
Validating activation key. This may take a few minutes...
Both Running and Flash permanent activation key was updated with the requested key.
```

As shown in Example 3-3, the system specifically notes a time-based key as such during the same activation process; you can see the remaining time before expiration as well.

### Example 3-3 *Successfully Activated Time-Based Key*

```
ciscoasa# activation-key d069a6c1 b96ac349 4d53caa7 d9c07b47 063987b5
Validating activation key. This may take a few minutes...
The requested key is a timebased key and is activated, it has 7 days remaining.
```

When you add a new time-based activation key that enables a single feature at the same level as another currently active key, the remaining time from the current key adds to the new key, as shown in Example 3-4. Keep in mind that both the current and new time-based keys must enable only one feature with the exact same capacity, if applicable; otherwise, the new key will deactivate and replace the current one.

### Example 3-4 *Time-Based Activation Key Aggregation*

```
ciscoasa# activation-key fa0f53ee a906588d 5165c36f f01c24ff 0abfba9d
Validating activation key. This may take a few minutes...
The requested key is a timebased key and is activated, it has 63 days remaining,
including 7 days from currently active activation key.
```

You can also deactivate a previously installed time-based license using the optional **deactivate** argument at the end of the **activation-key key** command, as shown in Example 3-5; this keyword is not available for the permanent activation key. After it is deactivated, the time-based key remains installed on the Cisco ASA. You can always reactivate this license later either manually or automatically upon the expiration of another time-based license.

### Example 3-5 *Deactivating a Time-Based Key*

```
ciscoasa# activation-key d069a6c1 b96ac349 4d53caa7 d9c07b47 063987b5 deactivate
Validating activation key. This may take a few minutes...
The requested key is a timebased key and is now deactivated.
```

In rare cases, the new permanent key that disables certain features may require a reload of the system before the change occurs. Example 3-6 shows the warning that the system displays before the strong encryption feature gets disabled by the new permanent license.

### Example 3-6 *Disabling a Feature with Reload Requirement*

```
ciscoasa# activation-key 6dlff14e 5c25a1c8 556335a4 fa20ac94 4204dc81
Validating activation key. This may take a few minutes...
The following features available in running permanent activation key are NOT
available in new permanent activation key:
  Encryption-3DES-AES
WARNING: The running activation key was not updated with the requested key.
Proceed with update flash activation key? [confirm]y
The flash permanent activation key was updated with the requested key,
and will become active after the next reload.
```

Because activation keys tie to a particular device using the serial number, it is possible to attempt to activate a key from one Cisco ASA on another; the software automatically checks for such errors and rejects an incorrect key. Example 3-7 illustrates such an attempt.

### Example 3-7 *Invalid Activation Key Rejected*

```
ciscoasa# activation-key 350ded58 7076f6c6 01221110 c67c806c 832ccf9f
Validating activation key. This may take a few minutes...
not supported yet.
ERROR: The requested activation key was not saved because it is not valid for this
system.
```

In older Cisco ASA Software versions, it is also possible for the system to reject an activation key when it contains unknown features. In Cisco ASA 8.2(1) and later software, all keys are backward compatible regardless of whether new features are present or not. For instance, when you downgrade from Cisco ASA 9.1(2) to 9.0(2) software with the IPS

Module license enabled, the same activation key remains valid after the downgrade even though the older software no longer supports this feature.

## Combined Licenses in Failover and Clustering

Prior to Cisco ASA Software version 8.3(1), both units in a failover pair required identical licensed feature sets. Given that most designs used the Active/Standby failover configuration, this led to underutilization of licensed capacities. After the changes in Cisco ASA 8.3(1) software, only the following license requirements remain for the ASA devices that participate in failover or clustering:

- For failover, Cisco ASA 5505, ASA 5510, and ASA 5512-X appliances must have the Security Plus license installed.
- For clustering, all participating Cisco ASA 5585-X appliances with SSP-10 and SSP-20 must have either the Base license or the Security Plus license. These have to match because all cluster members must have the 10GE I/O feature in the same state.
- For clustering, each Cisco ASA 5580 and ASA 5585-X unit must have the Cluster feature enabled independently. Cisco ASA 5500-X appliances require Cisco ASA 9.1(4) software to use this feature, and it is enabled by default on all Cisco ASA 5515-X, ASA 5525-X, ASA 5545-X, and ASA 5555-X models and on the Cisco ASA 5512-X with the Security Plus license.
- For both failover and clustering, all units must have the same encryption license. The Encryption-3DES-AES license must be in the same state on both failover peers and all cluster members.

After satisfying these basic requirements, the rest of the licensed features and capacities from both failover peers and all active cluster members combine to form a single feature set that all the participating devices use concurrently.

## License Aggregation Rules

The system follows these steps to create a combined feature set of a failover pair or a cluster:

1. Each failover unit or cluster member computes its local feature set by combining the permanent and active time-based activation keys using the rules discussed earlier.
2. For each feature that can be either enabled or disabled, the combined failover or cluster license inherits the best setting from all of the feature sets of the participating devices. For instance, each unit of a cluster enables the IPS Module license if at least one of the members has it enabled in the local feature set.
3. For each tiered feature, the licensed capacities of the individual units combine up to the platform limit of each member. This happens even if the particular tiered counts for the same feature do not match between all participating members. Consider a failover pair of Cisco ASA 5525-X appliances where both the primary and secondary

units have the active AnyConnect Premium Peers licenses for 500 sessions each. After aggregating these capacities, each device in this failover pair allows up to 750 sessions for this feature. Notice that the combined count of 1000 sessions from the individual licenses exceeds the Total VPN session count of 750 for this platform; this causes the downward adjustment.

After license aggregation, each failover peer or cluster member displays an additional section in the output of the **show version** and **show activation-key** commands to reflect the combined active feature set of the device. As shown in Example 3-8, this feature set supersedes the licensed feature set of the local unit as long as it continues to participate in a failover pair or a cluster.

**Example 3-8** *Aggregated Cisco ASA License Information with Failover or Clustering*

```
Failover cluster licensed features for this platform:
Maximum Physical Interfaces      : Unlimited      perpetual
Maximum VLANs                   : 1024          perpetual
Inside Hosts                     : Unlimited      perpetual
Failover                         : Active/Active  perpetual
Encryption-DES                   : Enabled        perpetual
Encryption-3DES-AES              : Enabled        56 days
Security Contexts                 : 4             perpetual
GTP/GPRS                          : Disabled       perpetual
AnyConnect Premium Peers         : 4             perpetual
AnyConnect Essentials            : Disabled       perpetual
Other VPN Peers                   : 10000         perpetual
Total VPN Peers                   : 10000         perpetual
Shared License                    : Disabled       perpetual
AnyConnect for Mobile            : Disabled       perpetual
AnyConnect for Cisco VPN Phone   : Disabled       perpetual
Advanced Endpoint Assessment     : Disabled       perpetual
UC Phone Proxy Sessions          : 54            56 days
Total UC Proxy Sessions          : 54            56 days
Botnet Traffic Filter             : Disabled       perpetual
Intercompany Media Engine        : Disabled       perpetual
10GE I/O                         : Enabled        perpetual
Cluster                          : Enabled        perpetual
```

This platform has an ASA5585-SSP-20 VPN Premium license.

If a device loses the connection to its failover peer or a cluster for over 30 days, it falls back to its locally licensed feature set. You can use the **clear configure failover** or **clear configure cluster** command to manually remove the aggregated license and force the unit to revert to its locally activated features before the 30-day period expires. This capability is useful when splitting failover or cluster members to configure them as shared VPN licensing peers instead.



## Aggregated Time-Based License Countdown

If the combined failover pair or cluster license relies on time-based activation keys to activate any features or aggregate licensed capacities, the countdown rules for these keys depend on the feature type:

- For any features that can be either enabled or disabled, only one participating unit continues the countdown at any given time. When this license expires, another device starts the countdown of its own time-based key for this feature. This way, the total licensed duration for this feature type combines from all applicable time-based activation keys in a failover pair or a cluster. Consider a failover pair where the primary unit has the Botnet Traffic Filter license for 52 weeks and the secondary unit has the same active license for 28 weeks. Only the primary Cisco ASA will continue the countdown of this license for the first 52 weeks of failover pair operation. After this activation key on the primary unit expires, the secondary unit will begin the countdown for another 28 weeks. As the result, you can benefit from the Botnet Traffic Filter feature in this failover pair without interruption for a combined duration of 80 weeks. If a unit loses communication with its failover peer or cluster for less than 30 days, the combined license still covers this period of independent operation for this device. If the interval of separation exceeds 30 days, the device subtracts the entire period from its local time-based license upon restoration of failover or cluster communication.
- Any time-based keys for tiered capacity features that contribute to the aggregated failover pair or cluster limits continue the countdown concurrently on their respective Cisco ASA units. Assume a cluster of four Cisco ASA 5580 appliances where each member has a 52-week license for ten virtual contexts in addition to the permanent key with two contexts. The combined license of the cluster allows configuring and using up to 48 virtual contexts for 52 weeks because all time-based tiered capacity licenses count down concurrently on all members. After 52 weeks, the combined cluster license drops down to eight security contexts based on the remaining permanent licenses of each member.

## Shared Premium VPN Licensing

It may become cost prohibitive to obtain multiple separate AnyConnect Premium Peers licenses if you manage a large number of Cisco ASA appliances that terminate SSL VPN, Clientless SSL VPN, and IPsec IKEv1-based remote-access VPN sessions. Even though individual appliances may reach the maximum expected number of concurrent VPN sessions at different times, it is unlikely that all of them will always remain at the peak load. Instead of obtaining a tiered AnyConnect Premium Peers capacity license to cover the worst-case scenario for each Cisco ASA in your network, you have the option of configuring your devices to share a pool of such licenses and request premium VPN session capacities as needed.

## Shared Server and Participants

To utilize a shared license pool for AnyConnect Premium sessions, you need to designate one Cisco ASA in the network as the shared licensing server. Other ASA devices that terminate AnyConnect Premium sessions become shared licensing participants. The server maintains the shared licenses and issues them to participants as necessary. You can optionally designate one participant ASA as the backup shared licensing server; this device will manage the shared pool only when the primary shared server becomes unavailable.

### Shared License

Like other licensed capabilities, the Shared License feature can be either enabled or disabled. However, it could also link with the tiered capacity of Shared AnyConnect Premium Peers when enabled. When the output of the **show version** or **show activation-key** command simply shows the Shared License feature as enabled, it means that the particular Cisco ASA can act as a shared licensing participant or a backup server. The same output from a shared licensing server also displays the associated quantity of shared licenses in the pool, as shown in Example 3-9.

#### Example 3-9 *Shared Server License*

Shared License	: Enabled	56 days
Shared AnyConnect Premium Peers	: 1000	perpetual

Keep in mind that the Shared AnyConnect Premium Peers license is not available separately from the Shared License feature; the particular activation key must enable this capability and specify the shared session capacity in order to enable a shared licensing server. You cannot use the regular AnyConnect Premium Peers license to provision or expand the shared session pool. Only the participant license can activate with a time-based activation key; the shared server license must use the permanent key.

### Shared Licensing Operation

After you install the appropriate licenses on the server and participants, you can configure these devices to share the licensed pool of AnyConnect Premium sessions. The server may also act as a participant without a separate license; it always uses the Shared AnyConnect Premium Peers capacity when terminating SSL VPN connections itself even if it has a regular AnyConnect Premium Peers license installed. Keep in mind that any Cisco ASA device may participate in a shared licensing domain under the following conditions:

- Each device has the Shared License feature enabled. Because hardware models do not have to match within a single domain, any device except a Cisco ASA 5505 can be the server or a participant.
- You configure each participant ASA with the same shared secret value as the licensing server.

- Each participant ASA has bidirectional IP reachability with the configured shared server and backup server, if applicable. The communication channel uses SSL encryption and allows crossing intermediate routers.

Each participant ASA follows this process when handling AnyConnect Premium connections:

1. Register with the shared licensing server, report the hardware model and local license information, and continue periodic polling over the communication channel.
2. Only when the system exhausts the local licensed capacity for AnyConnect Premium sessions, request additional session licenses from the shared pool in blocks of 50. The total count of locally licensed and shared sessions cannot exceed the Total VPN Sessions capacity for the platform. The server may not always provision the requested number of licenses if the remaining shared pool capacity is low.
3. Send to the server periodic refresh messages indicating that the requested allocation is still active. If the server does not hear from the participant within three consecutive refresh intervals, the allocation may expire. However, the participant continues using the allocated shared session count for up to 24 hours. If the communication channel with the server remains severed after this grace period, the device falls back to using the local licensed capacity; only new connections are affected. Even if the communication channel re-establishes within the 24-hour period, the same shared pool capacity may no longer be available on the server.
4. When the session count drops below the level that requires additional shared licenses, the client releases the allocated pool back to the server.

When you configure one of the participants to act as a backup shared licensing server, this unit must establish a communication channel to synchronize the pool information with the primary server first. When the primary licensing server goes down, the backup fully takes over the shared pool for up to 30 days of independent operation; the primary server resumes its normal duties after it comes back up. Upon initial synchronization, the backup server is only capable of five days of independent operation when the primary server goes offline; this period extends by one day every day up to the maximum of 30 days as long as the communication channel with the primary server remains operational. The following system log message is generated by the backup licensing server when the maximum allowed interval of independent operation is about to expire:

```
%ASA-4-444110: Shared license server backup has 15 days remaining as active license server.
```

Keep in mind that both peers in a failover pair have the exact same shared licensing role. In other words, you cannot configure the primary Cisco ASA as the shared licensing server and the secondary ASA as its backup. The secondary unit takes over as the primary licensing server after a failover event; you should configure some other ASA as the backup licensing server, if desired.

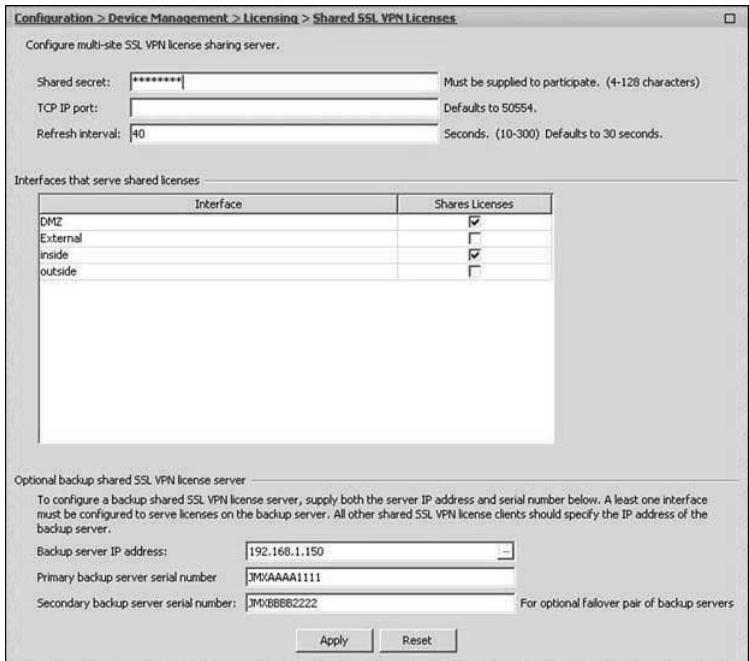
## Configuring Shared Licensing

You should have the following information ready before starting the configuration process of Shared Licensing:

- Shared secret key that the given shared licensing group will use.
- Identity of the designated primary shared licensing server and its IP addresses on every interface that will accept connections from participants.
- If applicable, the IP address and the serial number of the Cisco ASA that will act as the backup shared licensing server; if this device participates in failover, you need the serial number of the secondary unit as well.

## Licensing Server

Configure the primary licensing server through Cisco Adaptive Security Device Manager (ASDM) by navigating to **Configuration > Device Management > Licensing > Shared SSL VPN Licenses**. Figure 3-1 shows what the configuration panel looks like if the device has the appropriate license to act as the primary licensing server.



**Figure 3-1** Shared Premium VPN Licensing ASDM Configuration Pane

Follow these steps to configure the shared licensing server on this ASDM panel:

1. Set the shared secret. Configure the same value on all of the participants within the same shared licensing domain.
2. Optionally, set a particular TCP port that the participants would use to connect to the server. It is not recommended to change the default value of 50554.
3. Optionally, change the refresh interval that the participants use to regularly confirm the active status of a shared session count allocation. The server releases the allocation back into the shared pool if it does not hear from the participant for three times the configured refresh interval.
4. Enable participant connections on the respective local interfaces of the shared server. Keep in mind that a participant can only connect to the “closest” interface of the licensing server. If the server ASA can reach a particular participant on the DMZ interface, that participant cannot connect to the server’s inside interface instead.
5. Optionally, configure the IP address and the serial number of the Cisco ASA that will act as the backup shared licensing server. If this device has failover configuration, you need to specify the serial number of the failover peer as well.

## Participants

After you have configured the shared licensing server, configure each participant using the following steps:

1. Specify the address of the closest interface of the shared licensing server and the shared secret value with the `license-server` command. If you changed the default TCP port on the server, you need to specify it here as well. The command has the following syntax:

```
license-server address server-IP secret shared-secret [port tcp-port]
```

2. If applicable, specify the IP address of the backup shared licensing server:

```
license-server backup backup-server-IP
```

## Backup Licensing Server

To configure a participant to act as the backup licensing server, add the following command for each interface that would accept connections from other participants when the primary server is down:

```
license-server backup enable local-interface-name
```

## Monitoring Shared Licensing Operation

Use the **show shared license** command to monitor the communication between the shared license server and its participants. This command also displays information about the shared pool size and utilization as well as the local platform limits. The specific output depends on whether you are looking at the server or a participant. Example 3-10 illustrates a sample output from a shared licensing server.

### Example 3-10 Shared License Server Statistics

```
asa# show shared license

Shared license utilization:
  AnyConnect Premium:
    Total for network :    4500
    Available         :    4500
    Utilized          :         0
  This device:
    Platform limit   :    750
    Current usage    :         0
    High usage       :         0

Client ID           Usage  Hostname
FCH12345678        0      ASA-5555
```

## Summary

Every Cisco ASA device provides a very comprehensive feature set through a combination of basic capabilities and platform capacities to service any secure network. This chapter discussed license mechanisms for advanced security features that add additional layers of protection or accommodate more complex network designs. It also explained how to scale the Cisco ASA capabilities as your network grows by leveraging tiered capacity licenses for certain features. This chapter covered permanent and time-based activation keys that allow you to create and manage the appropriate feature set for any given Cisco ASA device. It provided an overview of how failover and clustering features enable aggregation of the licensed capacities to increase the efficiency of your investment. The final sections showed how you can group multiple ASA devices to service premium VPN sessions from a shared license pool.

# Index

## Numbers

---

10GE I/O feature, 62

## A

---

AAA (authentication, authorization, and accounting), 191, 227

accounting, configuring, 219-222

administrative connections, troubleshooting, 222-227

attributes, DAP (dynamic access policies), 1063-1065

*configuring, 204-209*

*configuring of administrative sessions, 204-209*

*firewall sessions, 209-214*

### authentication

authorization, configuring, 215-219

customizing authentication prompts, 214-215

protocols, 192-198

server group authentication protocols, 201

services, 192-198

support matrix, 192

### AAA Server Group

Authentication Protocols

example (7-1), 201

aaa-server command, 203

access control lists (ACLs). *See* ACLs (access control lists)

access deny message attribute (SSL VPN), 998

Access List to Allow Decrypted Traffic to Pass Through the ASA example (19-6), 817

Access List to Bypass NAT example (19-7), 818

Access Method tab (ASDM), 1073-1074

access policies, DAP (dynamic access policies), defining, 1068-1069

### accessing

ASDM (Adaptive Security Device Manager), 94-97

appliances, 81-87

*clientless remote-access SSL VPNs, configuring, 1034-1040*

Privileged and Configuration modes, 86

Accessing the Privileged and Configuration Modes example (4-3), 86

access-list option (match), 471

accounting, 191

configuring, 219-222

RADIUS (Remote Authentication Dial In User Service), 220

TACACS+ (Terminal Access Controller Access Control System Plus), 221-222

ACI (Application Centric Infrastructure), 27

ACLs (access control lists), 229, 243

characteristics, 231-232

comparing features, 234

downloadable, 254

*configuring, 218-219*

EtherType, 233

*configuring, 610-611*

extended, 233

ICMP filtering, 254-255

interface, transparent firewalls, 608-611

IPv6, configuring, 386-388

matching specific traffic, 468

monitoring, 260-265, 637

NAT (Network Address Translation), integration, 359-362

object grouping, 243-250

standard, 233, 250-251

time-based, 251-253

- Webtype, 234
- web-type, configuring, 1031-1034
- Action attribute (Add Access Rule dialog box), 235
- Action attribute (Add Management Access Rule), 241
- action option (transfer-encoding type command), 515
- Action tab (ASDM), 1068-1069
- Activating the Identity Certificate on the Outside Interface example (22-4), 993
- activation key option (system execution space), 534
- activation keys
  - combining, 69-70
  - invalid, 72
  - managing licenses, 68-73
  - permanent, 68-70
  - time-based, expiration, 70-71
  - using, 71-73
- Active Directory, Kerberos, 197
- Active/Active failover, 654-656
  - asymmetric routing, 662-664
- Active/Standby failover, 654-656
  - deployment scenario, 680-684
- ActiveX relay attribute (SSL VPN), 998
- AD agent, connecting to, 312-313
- Adaptive Inspection and Prevention Security Services Module (AIP-SSM) models, 53-54
- Adaptive Security Device Manager (ASDM), 82
- Add AAA Server dialog box, 199
- Add Access Rule dialog box, 235-236
- Add Authentication Rule dialog box, 210
- Add Authorization Rule dialog box, 215-216
- Add Automatic Address Translation Rules attribute (Add Network Object dialog box), 351
- Add Customization Object dialog box, 1009
- Add DNS Inspect dialog box, 478
- Add Identity Certificate dialog box, 938
- Add Management Access Rule dialog box, 241-242
- Add NAT Rule dialog box, 366, 368, 370-371
- Add Network Object dialog box, 351-352, 363, 365
- Add Signature dialog box, 756-758
- Adding New Local CA Users Through the CLI example (21-25), 965
- Adding User Contexts in System Execution Space example (14-6), 549
- Address Assignment from a DHCP Server example (20-9), 884
- address translation
  - see also* NAT (Network Address Translation); PAT (Port Address Translation)
  - behavior, 346-350
  - configuring, 350-371
  - dynamic NAT/PAT, 343-344
  - enabling, 1116
  - identity NAT, 344
  - monitoring, 375-377
  - NAT (Network Address Translation), 3-4, 338-340, 377
  - ACL (*access control lists*) integration, 359-362
  - auto configuration*, 351-355
  - bypassing*, 817-818
  - clustering*, 698-700
  - configuration use cases*, 362-371
  - manual configuration*, 356-359
  - transparent firewall restrictions*, 600-602
- PAT (Port Address Translation), 4-5, 340
- policy NAT/PAT, 344
- redesigning, 349-350
- security protection mechanisms, 345-346
- static, 5-6
- static NAT/PAT, 341-342
- addresses
  - IPv6, 380-382
    - assigning*, 383-384
    - translation*, 389-390
  - pools, defining, 1101-1103
- admin context, virtual firewall, 535
  - configuring, 552-553, 563-568
- Administration section (PRSM interface), 286
- administrative connections, troubleshooting, 222-227
- administrator accounts, IPS (intrusion prevention system), 769
- ADSM (Adaptive Security Device Manager), 82
  - adding default routes, 392
  - adding static routes, 392
- Advanced Endpoint Assessment feature, 64
  - configuring, 1058-1059
  - Host Scan, 1055
- Advanced Inspection and Prevention Security Services Module (AIP-SSM). *See* AIP-SSM (Advanced Inspection and Prevention Security Services Module)



- Advanced NAT Settings dialog box, 352-353, 363-364, 365, 368, 370
- advanced security features, 63-65
  - Advanced Endpoint Assessment, 64
  - AnyConnect for Cisco VPN Phone, 64
  - AnyConnect for Mobile, 64
  - Botnet Traffic Filter, 64
  - Cluster, 64-65
  - GTP/GPRS, 64
  - Intercompany Media Engine, 63-64
  - IPS Module, 65
- Aggregated Cisco ASA License Information with Failover or Clustering example (3-8), 74
- aggregation
  - licenses, rules, 73-74
  - time-based activation keys, 71
- AIP-SSM (Adaptive Inspection and Prevention Security Services Module), 29
  - models, 53-54
- Alert Notes parameter (Add Signature dialog box), 758
- Alert Severity parameter (Add Signature dialog box), 757
- algorithms, support, 129
- all FTP command, 485
- Allocating Interfaces to a User Context example (14-8), 550
- allow option
  - content-length command, 510
  - max-header-length command, 512
  - max-uri-length command, 512
  - port-misuse command, 512
  - request-method command, 514
  - strict-http command, 510
  - transfer-encoding type command, 515
- Allowing VPN Clients for Internet Access example (20-23), 901
- anomaly detection, IPS (intrusion prevention system), 763-766
- anomaly-based analysis, 12-14
- Anti-Spyware endpoint attribute (DAP), 1067
- AntiSpyware scans, Host Scan, configuring, 1059
- Anti-Virus endpoint attribute (DAP), 1067
- antivirus host scans, Host Scan, configuring, 1059
- any option (match), 471
- AnyConnect client
  - configuring, 1109-1112
  - deploying, 1112-1116
- AnyConnect endpoint attribute (DAP), 1067
- AnyConnect Essentials, 66
  - license, SSL VPNs, 984
- AnyConnect for Cisco VPN Phone feature, 64
- AnyConnect for Mobile feature, 64
- AnyConnect Premium Peers feature, 66
- AnyConnect Secure Mobility Client, 25-26
  - AnyConnect client, configuring, 1109-1112
  - configuring, 1096-1112
  - defining attributes, 1098-1103
  - loading, 1096-1098
  - tunneling features, 1103-1109
- AnyConnect SSL VPNs
  - configuring, 1115-1116
  - license, 984
  - troubleshooting, 1116-1118
- AnyConnect tab (ASDM), 1074
- appe FTP command, 485
- appliances, accessing, 81-87
  - clientless remote-access SSL VPNs, configuring, 1034-1040
- Application Centric Infrastructure (ACI), 27
- Application endpoint attribute (DAP), 1067
- Application Inspection Engine module (CX), 276
- application inspections, 465-468
  - Cisco Unified Communications (UC) advanced support, 499-506
  - CTIQBE (Computer Telephony Interface Quick Buffer Encoding), 473-475
  - Distributed Computing Environment Remote Procedure Calls (DCERPC), 476
  - DNS (Domain Name System), 476-480
  - enabling, 468-469
  - ESMTP (Extended SMTP), 481-483
  - FTP (File Transfer Protocol), 484-486
  - GPRS (General Packet Radio Service), 486-492
  - GTP (GPRS Tunneling Protocol), 489-490
  - H.323, 492-499
  - HTTP inspection engine, 507-515
  - ICMP (Internet Control Message Protocol) packets, 515-516
  - ILS (Internet Locator Service), 516
  - IM (Instant Messenger), 517-518
  - IPsec pass-through, 518-519
  - MGCP (Media Gateway Control Protocol), 519-521

- NetBIOS, 521
- PPTP (Point-to-Point Tunneling Protocol), 522
- RSH (Remote Shell), 523
- RTSP (Real-Time Streaming Protocol), 523-524
- SCCP (Simple Client Control Protocol), 525-527
  - selective, 469-473
- SIP (Session Initiation Protocol), 524-525
- SNMP (Simple Network Management Protocol), 527-528
- SQL\*Net, 528
- Sun Remote Procedure Call (RPC), 522-523
  - supported, 467-468
- TFTP (Trivial File Transfer Protocol), 528
- WAAS (Wide Area Application Services), 528
- XDMCP (X Display Manager Control Protocol), 529
- application objects (CX), 299-300
- application proxies, 3
- Application Types dashboard (CX), 330
- Application Visibility and Control component (Data Plane), 275
- Applications dashboard (CX), 330
- application-service objects (CX), 303-304
- Applying a Crypto Map to the Outside Interface example (20-12), 885
- Applying QoS on the Outside Interface example (25-9), 1155
- Applying Signature Updates example (17-4), 774
- architecture
  - CSD (Cisco Secure Desktop), 1045-1046
  - CX (ConteXt Security) modules, 273-277
    - Application Inspection Engine*, 276
    - Control Plane module*, 276-277
    - Data Plane module*, 274-275
    - Evening and Reporting module*, 275
    - HTTP Inspection Engine module*, 276
    - Management Plane module*, 276
    - TLS (Transport Layer Security) Decryption Proxy module*, 276
    - User Identity module*, 275
  - DAP (dynamic access policies), 1061-1062
  - logical, IPS (intrusion prevention system), 735
  - QoS (Quality of Service), 1136-1142
  - virtual firewall, 533-544
- ARP (Address Resolution Protocol), transparent firewalls, enabling inspection, 613-615
- ARR metric (RR), 791
- ASA (Adaptive Security Appliance)
  - configuring, for IPS traffic redirection, 778-780
  - 5500-X Series Next-Generation Firewall, 57
    - CLI (command-line interface)*, 90-92
    - parameters and values*, 91
  - initial setup, 90-100
    - management (PRSM), 283
  - ASA EtherChannel Configuration in Individual Mode example (16-16), 696
  - ASA IPS Image Recovery Process Debug example (17-1), 746
  - ASA Services Module (ASASM), 173
    - ASA's Full Configuration Showing QoS for VoIP, Mail, and Web example (25-10), 1160-1162
    - ASA's Full Configuration Using Inbound and Outbound ACLs example (8-9), 259-260
    - ASASM (ASA Services Module), 51, 173-176, 189
      - deployment scenarios, 180-183
      - edge protection, 182-183
      - hardware architecture, 174-175
      - host chassis
        - integration*, 175-176
        - managing*, 176-180
      - internal segment firewalling, 181-182
      - trusted flow bypass with policy-based routing, 183-189
    - ASASM Initialization Message on Chassis example (6-1), 176
    - ASDM (Adaptive Security Device Manager)
      - AAA (authentication, authorization, and accounting) test utility, 226-227
      - Access Method tab, 1073-1074
      - accessing, 94-97
      - Action tab, 1068-1069
      - AnyConnect tab, 1074
      - ASA CX Status tab, 97
      - Bookmarks tab, 1073
      - configuration, 98-99, 257-259
      - connections, authentication, 208-209
      - Content Security tab, 97
      - Device Dashboard tab, 96-97
      - enabling RIP in, 401
      - Firewall Dashboard tab, 97
      - Functions tab, 1071

- image upgrade, 133-136
  - initial setup, 92-100
  - Intrusion Prevention tab, 97
  - Local CA (Certificate Authority)
    - configuring*, 958-960
    - enrolling users through*, 963-965
  - logging, 150
  - monitoring IPS, 793
  - Monitoring screen, 99-100
  - Network ACL Filters tab, 1069
  - PKI (Public Key Infrastructure) certificates, installing, 936-938
  - Port Forwarding Lists tab, 1072
  - QoS (Quality of Service), configuring, 1143-1151, 1157-1160
  - setting up for IPS management, 752
  - uploading, 92-93
  - Webtype ACL Filters tab, 1070-1071
  - ASR metric (RR), 790
  - assigned IP address AAA attribute, 1063
  - assigning
    - IP addresses, 606
    - IPv6 addresses, 384
    - VLAN interfaces, 177-178
    - Management IP addresses, 606
  - Assigning a Management IP Address example (15-6), 606
  - Assigning an IP Address example (15-5), 606
  - Assigning IPv6 Addresses example (11-1), 384
  - asymmetric routing groups, failover, 662-664
  - Attack Response Controller (IPS), 742
  - attributes
    - AnyConnect Secure Mobility Client, defining, 1098-1103
    - IPsec, 20, 804
    - ISAKMP, 802
    - SSL VPNs, configurable, 998
  - auth event class, 148
  - authentication, 191
    - see also* AAA (authentication, authorization, and accounting)
    - ASDM connections, 208-209
    - authentication server, defining, 198-204
    - client-based remote-access SSL VPNs, 1094-1095
    - configuring, 204-209
      - administrative sessions*, 204-209
    - customizing, 214-215
    - EIGRP, 447-448
    - firewall sessions, cut-through proxy feature, 209-214
    - IPsec remote-access VPNs, 907-909
    - OSPF (Open Shortest Path First), configuring, 422-426
    - RADIUS (Remote Authentication Dial In User Service), 194-195
      - accounting*, 220
      - setting up*, 1114-1115
    - RIP (Routing Information Protocol), 403-406
    - SecurID (SDI), 196-197
    - serial console connections, 207-208
    - server group authentication protocols, 201
    - service support, 192
    - SSH (Secure Shell) connections, 206-207
    - SSL VPNs, configuring, 987-1004
    - Telnet connections, 204-206
    - timeouts, 214
    - user identity services, tuning settings, 313-314
  - authentication, authorization, and accounting (AAA). *See* AAA (authentication, authorization, and accounting)
  - authentication server, defining, 198-204
  - AuthenticationApp (IPS), 741
  - authorization, 191
    - see also* AAA (authentication, authorization, and accounting)
    - commands, 217-218
    - configuring, 215-219
    - service support, 193
  - auth-prompt command, 215
  - Automatic Saving of Logs in Flash example (5-31), 155
  - Automatic Saving of Logs in the FTP Server example (5-32), 156
  - Available DSCP Options in Class Maps example (25-1), 1140
- ## B
- 
- backing up IPS (intrusion prevention system) configuration, 776
  - Backing Up CIPS Configuration to FTP Server example (17-5), 776
  - banner attribute (SSL VPN), 998
  - banner option (system execution space), 534
  - Base License, 59-60
  - Basic ASASM Interface Configuration example (6-9), 186
  - Basic Chassis Configuration example (6-10), 186
  - Basic CLI OSPF Configuration example (12-13), 418
  - Basic Failover Configuration on Primary Unit example (16-5), 670
  - Basic Failover Configuration

- on Secondary Unit example (16-6), 671
- Basic Host Scan, 1055
  - configuring, 1057-1058
- Basic Management
  - Configuration on Master Unit example (16-19), 709
- Basic Management
  - Configuration on Slave Unit example (16-20), 709
- basic platform capabilities, 61-63
- behavior, address translation, 346-350
- blacklist data, BTF (Botnet Traffic Filter), dynamic and local, 781-782
- bookmark list attribute (SSL VPN), 998
- bookmarks, clientless remote-access SSL VPNs, configuring, 1024-1031
- Bookmarks tab (ASDM), 1073
- boot option (system execution space), 534
- Botnet Traffic Filter (BTF). *See* BTF (Botnet Traffic Filter)
- bridge event class, 148
- browsers, SSL VPNs, requirements, 986-987
- BTF (Botnet Traffic Filter), 64, 780-786
  - blacklist data, dynamic and local, 781-782
  - DNS snooping, 782-783
  - icon (Monitoring screen), 100
- traffic selection, 783-786
- buffered logging, 151-152
- buffers, sizes, 166
- bypassing NAT, site-to-site IPsec VPNs, 817-818
- bytes option
  - content-length command, 510

- max-header-length command, 512
- max-uri-length command, 512

## C

---

- CA (Certificate Authority), 933-935
  - importing certificates manually, 989
  - installing certificates from files, 937-938
- Local CA (Certificate Authority), 957-966
  - configuring with ASDM*, 958-960
  - configuring with CLI*, 960-963
  - enrolling users through ASDM*, 963-965
  - enrolling users through CLI*, 965-966
- ca event class, 148
- Cache Cleaner, CSD (Cisco Secure Desktop), 1043-1044
- capture command, 638-639
- capturing packets, 169-171
  - CX (ConteXt Security) modules, 332-335
- Capturing Traffic Toward ASASM with SPAN example (6-8), 180
- CDA (Cisco Context Directory Agent), 275
  - connecting to, 312-313
- cdup FTP command, 485
- centralized connection processing, cluster packet flow, 702-703
- centralized license management (PRSM), 283
- Certificate Authority (CA). *See* CA (Certificate Authority)
- Certificate Enrollment Invitation Email example (21-24), 965

- certificates, 932-933
  - CA (Certificate Authority), 933-935
    - importing certificates manually*, 989
    - installing certificates from files*, 937-938
  - Local CA (Certificate Authority)*, 957-966
- Cisco ASA, configuring to accept remote-access IPsec VPN clients, 971-972
- client-based remote-access SSL VPNs, digital certificates, 1090
- configuring IPsec site-to-site tunnels, 966-971
- CRLs (certificate revocation lists), 935-936
- digital, enrolling, 988-993
- identity certificates, identity
  - installing from a file*, 938
  - installing using SCEP*, 943-945
  - manually importing*, 993
- installing, 936-957
  - CA by copy-and-paste*, 939
  - CLI (command-line interface)*, 945-957
  - SCEP (Simple Certificate Enrollment Protocol)*, 940-943
  - through ASDM*, 936-938
- SCEP (Simple Certificate Enrollment Protocol), 936
- troubleshooting, 972-977
- Changing the Default Physical Media Type to Nonbroadcast example (12-22), 432
- Changing to a User Context example (14-13), 554
- Changing to an Admin Context example (14-10), 552
- Chassis MAC Address Table

- for Firewall Backplane Link example (6-7), 179-180
- Checking ASA IPS Module Installation Status example (9-2), 277
- Checking the Interfaces for ARP Inspection example (15-20), 637
- Checking the L2F Table example (15-19), 636
- CIPS (Cisco Intrusion Prevention System)
  - accessing CLI, 747-748
  - displaying, 771-772
  - installing, 744-747
  - IPS (intrusion prevention system), configuring on, 753-768
  - license key installation, 752-753
  - troubleshooting, 1082
  - upgrading, 772-776
- CIPS Version and Process Information example (17-3), 771
- cipsWebserver (IPS), 742
- Cisco 5505 Easy VPN Client Configuration example (20-17), 895-896
- Cisco AnyConnect Secure Mobility Client. *See* AnyConnect Secure Mobility Client
- Cisco ASA 1000V Cloud Firewall, 26-27, 52-53
- Cisco ASA 5500 Firewall, 57
  - models, 30-31
    - Cisco ASA 5505*, 30-34
    - Cisco ASA 5510*, 35-37
    - Cisco ASA 5520*, 41
    - Cisco ASA 5540*, 42-44
    - Cisco ASA 5550*, 45-46
- Cisco ASA 5500-X Series 6-Port GE Interface cards, 57
- Cisco ASA 5500-X Series Next-Generation Firewall models, 30-31
  - Cisco ASA 5512-X*, 38-39
  - Cisco ASA 5515-X*, 40
  - Cisco ASA 5525-X*, 42
  - Cisco ASA 5545-X*, 42-45
  - Cisco ASA 5555-X*, 45
  - Cisco ASA 5585-X Series*, 47-51
- Cisco ASA 5580 expansion cards, 56-57
- Cisco ASA CX, 53
- Cisco ASA Gigabit Ethernet Modules, 55-57
- Cisco ASA License Information example (3-1), 67-68
- Cisco ASA Next-Generation Firewall Services, 53
- Cisco ASA Phone Proxy feature, 500-504
- Cisco ASA SSM-4GE, 55
- Cisco ASA's Relevant Configuration for Site-to-Site IPsec Tunnel example (19-18), 833-836
- Cisco ASA's Relevant Configuration to Allow IP Traffic example (15-16), 622-623
- Cisco ASA's Relevant Configuration with Multiple Security Contexts example (14-18), 569-572
- Cisco ASA's Relevant Configuration with Multiple Security Contexts example (14-19), 582-585
- Cisco ASA's Relevant Configuration with Multiple Security Contexts example (15-17), 632-636
- Cisco Context Directory Agent (CDA), 275
- Cisco Secure Desktop (CSD). *See* CSD (Cisco Secure Desktop)
- Cisco Unified Communications (UC)
  - advanced support, application inspections, 499-506
- citrix event class, 148
- class maps, QoS (Quality of Service), setting up, 1152-1153
- Class Maps to Identify Mail and VoIP Traffic example (25-3), 1153
- Class Maps to Identify Tunnel Traffic example (25-4), 1153
- class Syslog Commands example (22-18), 1080-1081
- classes, event, 148
- classification, packet, virtual firewall, 536-541
- clear access-list counters command, 261
- Clearing All ikev1 Commands from the Running Configuration example (5-8), 125
- Clearing IPS EventStore example (17-6), 778
- Clearing the DF Bit for IPsec Packets example (19-17), 830
- Clearing the L2F Table Associated with the Outside Interface example (15-26), 639
- Clearing the Running Configuration example (5-9), 125
- Clearing the Startup Configuration example (5-10), 126
- CLI (command-line interface), 81, 85-87, 118
  - AAA (authentication, authorization, and accounting) test utility, 226-227
  - CIPS system software, accessing, 747-748
  - configuring AAA server, 201
  - defining management access rule, 241
  - displaying routing tables, 399-400
  - filtering incoming RIP routes, 408
  - initial setup, 90-92

- installing PKI certificates from, 945-957
- Local CA (Certificate Authority) users, enrolling, 965-966
- QoS (Quality of Service), configuring, 1152-1155, 1157-1160
- Split tunneling, 1105
  - tracing packet flow, 168-169
- CLI Commands for Filtering Incoming RIP Routes example (12-6), 408**
- CLI Split Tunneling Configuration example (23-7), 1105**
- client firewalling, IPsec remote-access VPNs, 904-907**
- client operating systems**
  - client-based remote-access SSL VPNs, requirements, 1088-1089
  - SSL VPNs, requirements, 986-987
- client-based remote-access SSL VPNs, 1085, 1118**
  - AnyConnect secure mobility client
    - configuring, 1096-1112*
    - deploying, 1112-1116*
    - licenses, 1086*
  - configuring, 1090-1095
  - deploying, 1086-1088
  - design considerations, 1086-1088
  - digital certificates, enrolling, 1090
  - group policies, configuring, 1090-1094
  - prerequisites, 1088-1090
  - troubleshooting, 1116-1118
  - tunnel policies, 1090-1094
  - user authentication, setting up, 1094-1095
- clientless connections, defining, 1076-1077**
- clientless remote-access SSL VPNs, 979-980, 1084**
  - application access, configuring, 1034-1040
  - bookmarks, configuring, 1024-1031
  - clientless connections, defining, 1076-1077
  - client-server plug-ins, configuring, 1040-1041
  - configuring, 1004-1041
  - CSD (Cisco Secure Desktop), 1041-1053
    - architecture, 1045-1046*
    - components, 1043-1044*
    - configuring, 1046-1053*
    - requirements, 1044-1045*
  - DAP (dynamic access policies), 1060-1074
    - architecture, 1061-1062*
    - configuring, 1062-1074*
    - sequence of events, 1062*
  - deploying, 1075-1078
  - design considerations, 980-982
  - enabling on interfaces, 1005-1006
  - Host Scan, 1054-1060
    - configuring, 1056-1060*
    - modules, 1054-1055*
  - licenses, 983-986
  - monitoring, 1078-1081
  - portal customization, configuring, 1006-1024
  - prerequisites, 982-987
  - smart tunnels, configuring, 1037-1040
  - troubleshooting, 1081-1084
  - web-type ACLs, configuring, 1031-1034
- client-server plug-ins, clientless remote-access SSL VPNs, configuring, 1040-1041**
- cloud computing, security, 26-27**
- Cluster feature, 64-65**
- Cluster Interface Mode**
  - Selection example (16-18), 708
- Cluster State Transition History example (16-25), 719**
- clustering, 685-731**
  - combined licenses, 73-75
  - configuring, 706-716
  - connection processing, 702-705
  - control interface, 690-697
  - data interface, 690-697
  - versus failover, 685
  - hardware requirements, 687-690
  - health monitoring, 697-698
  - individual mode, 695-697
  - license aggregation, 685
  - monitoring, 717-720
  - NAT (Network Address Translation), 698-700
  - packet flow, 702-706
  - performance, 700-702
  - software requirements, 687-690
  - spanned EtherChannel deployment, 720-731
  - spanned EtherChannel mode, 693-695
  - state transition, 705-706
  - stateful connection redundancy, 685
  - troubleshooting, 717-720
  - unit roles, 685-687
  - Zero Downtime upgrade, 688-689
- clustering option (system execution space), 534**
- Cluster-Spanned EtherChannel Configuration example (16-22), 716**
- Cluster-wide EtherChannel Information example (16-26), 720**
- CollaborationApp, IPS**

- (intrusion prevention system), 744
- Complete Basic Cluster
  - Configuration on Master Unit example (16-21), 712
- Complete Cluster
  - Configuration on Master Unit example (16-27), 729-731
- Complete Failover
  - Configuration on Primary example (16-15), 684
- Complete Floating Static Route Configuration with Tracking example (16-3), 652
- Components section (PRSM interface), 286
- Computer Telephony Interface Quick Buffer Encoding (CTIQBE) inspections, 473-475
- config event class, 148
- configuration
  - accounting, 219-222
  - ACE, 249
  - ACLs (access control lists), 11.101-11.111
    - basic, 251
    - EtherType, 610-611
    - extended, 240
    - address translation, 350-371
    - Aironet LEAP bypass, 909
    - AnyConnect Secure Mobility Client, 1096-1112
  - ASA, accepting remote-access IPsec VPN clients with certificates, 971-972
  - ASDM, 257-259
  - authentication, 204-209, 908
    - HTTP for ASDM, 209
    - Serial console, 208
    - SSH to a TACACS+ server, 207
  - authorization, 215-219
  - CA (Certificate Authority), Local CA, 960
  - central protection policy, 906-907
  - certificate lifetimes, 961
  - client-based remote-access SSL VPNs, 1090-1095
  - clientless remote-access SSL VPNs, 1004-1041
    - application access, 1034-1040
    - client-server plug-ins, 1040-1041
    - web-type ACLs, 1031-1034
  - clustering, 706-716
  - CSD (Cisco Secure Desktop), 1046-1053
  - CX (ConteXt Security) modules, preparing for, 277-282
  - CX policy element headers, 294
  - DAP (dynamic access policies), 1062-1074, 1077-1078
  - DHCPv6 relay functionality, 385
  - DNS Doctoring, 375
  - downloadable ACLs (access control lists), 218-219
  - EIGRP, 441-453
    - MD5 authentication using CLI, 448
    - route filtering via the CLI, 447
    - static neighbor, 448
    - summary address, 449
  - email logging, 154
  - failover, 667-678
  - Host Scan, 1056-1060
  - IP multicast routing, 1120-1127
  - IP Phone bypass, 909
  - IPS (intrusion prevention system)
    - backing up, 776
    - basic management settings, 748-752
    - CIPS, 753-768
    - preparing for, 744-753
    - traffic redirection, 778-780
  - IPsec remote-access VPNs
    - IKEv1 configuration, 862-889
    - IKEv2 configuration, 889-896
  - IPsec site-to-site tunnels, PKI certificates, 966-971
  - IPv6, 382-390
  - L2TP over IPsec remote-access VPN, configuring, 912-915
  - Local CA (Certificate Authority)
    - ASDM, 958-960
    - CLI (command-line interface), 960-963
  - management, 119-126
  - management-only interface, 111
  - NAT (Network Address Translation)
    - automatic, 351-355
    - manual, 356-359
    - static translation, 611
    - use cases, 362-371
  - NetFlow, 158-159
  - NTP server, 118
  - OSPF (Open Shortest Path First), 413-419
    - authentication, 422-426
    - redistribution, 426-427
  - PBR (policy-based routing), 185-189
  - PFS DH-Group 5 for a peer, 820
  - PIM RP, 1126
  - QoS (Quality of Service), 1142-1155
    - via ASDM, 1143-1151, 1157-1160
    - via CLI (command-line interface), 1152-1155, 1157-1160
  - redundant interfaces, 644-645
  - removing, 124-126
  - RIP (Routing Information

- Protocol), 401-403
- running, 119-123
- server-based object groups, 247-248
- site-to-site IPsec VPNs, 805-822
  - traffic filtering*, 816-817
- SMTP server, 960
- SSL VPNs
  - authentication*, 987-1004
  - group policies*, 994-998
  - tunnel groups*, 997-1000
- startup, 123-124
- static IP routes, 392-400
- traffic filtering, 235-242
- transparent firewalls, 602-616
  - adding static L2F table entries*, 612
  - enabling ARP inspection*, 613-615
  - guidelines*, 602-603
  - interface ACLs*, 608-611
  - interfaces*, 604-605
  - IP addresses*, 605-606
  - modifying L2F table parameters*, 615-616
  - NAT (Network Address Translation)*, 611-612
  - routes*, 606-607
- trustpoints, 946
- virtual firewall, security contexts, 544-559
- configuration database (CX), backup, 292-293
- Configuration of a Standard ACL example (8-5), 251
- Configuration of an ACE Using Object Groups example (8-4), 249
- Configuration of an Extended ACL example (8-1), 240
- Configuration of Central Protection Policy example (20-25), 906-907
- Configuration of Cisco Aironet LEAP Bypass example (20-29), 909
- Configuration of Cisco IP Phone Bypass example (20-30), 909
- Configuration of Data Interfaces in Transparent Firewall example (15-4), 605
- Configuration of DNS Doctoring example (10-16), 375
- Configuration of Email Logging example (5-30), 154
- Configuration of Individual User Authentication example (20-27), 908
- Configuration of Individual User Idle Timeout example (20-28), 908
- Configuration of Interactive Client Authentication example (20-26), 908
- Configuration of NTP Server example (4-18), 118
- Configuration of Priority Queue example (25-2), 1152
- Configuration of Reverse Route Injection example (19-10), 824
- Configuration of Server-Based Object Group example (8-3), 247-248
- Configuration of Telnet Access on the Management Interface example (5-11), 128
- Configuration of Use Case 1 in Pre-8.3 Version of Software example (10-7), 364
- Configuration of Use Case 1 in Version 8.3 and Later Software example (10-6), 364
- Configuration of Use Case 2 in Pre-8.3 Version of Software example (10-9), 365
- Configuration of Use Case 2 in Version 8.3 and Later Software example (10-8), 365
- Configuration of Use Case 3 in Pre-8.3 Version of Software example (10-11), 367
- Configuration of Use Case 3 in Version 8.3 and Later Software example (10-10), 367
- Configuration of Use Case 4 in Pre-8.3 Version of Software example (10-13), 369
- Configuration of Use Case 4 in Version 8.3 and Later Software example (10-12), 369
- Configuration of Use Case 5 in Pre-8.3 Version of Software example (10-15), 371
- Configuration of Use Case 5 in Version 8.3 and Later Software example (10-14), 371
- Configuration screen (ASDM), 98-99
- Configuration to Allow NEM example (20-31), 910
- Configuration to Load-Balance Cisco IPsec Clients with Site-to-Site VPN example (20-32), 919-922
- Configurations section (PRSM interface), 285
- Configuring a Description on the Security Context example (14-7), 549
- Configuring a Management-Only Interface example (4-15), 111
- Configuring a PIM RP example (24-6), 1126
- Configuring a Static EIGRP Neighbor example (12-37), 448
- Configuring a Static NAT



- Translation example (15-10), 611
- Configuring a Trustpoint example (21-4), 946
- Configuring an EIGRP Summary Address example (12-38), 449
- Configuring an EtherType ACL (15-9), 610-611
- Configuring and Applying an IPv6 ACL on the Outside Interface example (11-4), 388
- Configuring and Applying an IPv6 ACL on the Outside Interface example (11-5), 390
- Configuring Authentication Exceptions by Using MAC Address Lists example (7-12), 213
- Configuring Certificate Lifetimes example (21-19), 961
- Configuring Cisco ASA for Manual Enrollment example (22-2), 991
- Configuring Cut-Through Proxy Using the CLI example (7-10), 211
- Configuring DHCP Service on the Inside Interface example (4-16), 113
- Configuring DHCPv6 Relay Functionality example (11-2), 385
- Configuring EIGRP MD5 Authentication Using the CLI example (12-36), 448
- Configuring EIGRP Route Filtering via the CLI example (12-35), 447
- Configuring Firewall Session Authentication Exceptions example (7-11), 212
- Configuring HTTP Authentication for ASDM Users example (7-9), 209
- Configuring Interfaces on ASA Services Module example (6-5), 178
- Configuring NetFlow via CLI example (5-34), 158-159
- Configuring PFS DH-Group 5 for a Peer example (19-8), 820
- Configuring Serial Console Authentication example (7-8), 208
- Configuring Speed and Duplex on an Interface example (4-11), 105
- Configuring SSH Authentication to a TACACS+ Server example (7-7), 207
- Configuring the AAA Server Using the CLI example (7-2), 201
- Configuring the ASA to Enroll via SCEP example (21-5), 948
- Configuring the Cisco ASA for Manual Enrollment example (21-9), 952
- Configuring the Local CA Using the CLI example (21-17), 960
- Configuring the SMTP Server example (21-18), 960
- connection events, CX (ConteXt Security) modules, 331-332
- Connection Profile AAA attribute, 1063
- console
  - establishing connections, 82-85
  - logging, 150
  - port settings, 84
- content area, SSL VPNs, 1014
- content-length command, 510
- content-type-verification command, 511
- Context A Configuration with ASR Groups example (16-9), 677
- Context B Configuration with ASR Groups example (16-10), 677-678
- context-aware access policies, CX (ConteXt Security) modules, defining, 324-327
- control interface, clustering, 690-697
- Control Plane module (CX), 276-277
- copy running-config startup-config command, 124
- Copying a System Image from a TFTP Server to the Local Flash example (5-13), 134
- Copying a System Image from an FTP Server to the Local Flash example (5-14), 134
- Copying the Running Configuration to NVRAM example (5-17), 135
- copyright area, SSL VPNs, 1011
- CPUs (central processing units)
  - monitoring, 165-168
  - troubleshooting, 172
  - utilization traps, 162
- Creating a Subinterface example (4-13), 108
- Creating an EtherChannel example (4-14), 110-111
- Creating an ISAKMP IKEv2 Policy example (19-2), 808
- Creating an ISAKMP Policy example (20-2), 874
- CRL Checking Example (21-14), 955
- crl configure Subcommand example (21-13), 955
- CRL Manual Retrieval via the CLI example (21-16), 957
- CRLs (certificate revocation lists)
  - checking, 955
  - manual retrieval via the CLI, 957
  - PKI (Public Key Infrastructure), 935-936
  - retrieval problems, troubleshooting, 975-976
- Crypto Map Configuration example (19-5), 815

- Crypto Map Configuration example (21-29), 968
- crypto maps, creating, 812-816, 884-885
- CSD (Cisco Secure Desktop)
  - architecture, 1045-1046
  - assigning policy, 1051
  - Cache Cleaner, 1043-1044
  - clientless remote-access SSL VPNs, 1041-1053
  - configuring, 1046-1053
  - host emulators, identifying, 1052-1053
  - Host Scan, 1054-1060
  - keystroke loggers, identifying, 1052-1053
  - prelogin policies, defining, 1048-1051
  - prelogin sequences, defining, 1048
  - registry checks, setting up, 1114
  - requirements, 1044-1045
  - Secure Desktop, 1043
  - Secure Desktop Manager, 1043
  - troubleshooting, 1083
- csd event class, 148
- CSM Event Manager, monitoring IPS, 794
- CSM Event Viewer, event tables, removing false positive IPS events, 794
- CTIQBE (Computer Telephony Interface Quick Buffer Encoding) inspections, 473-475
- CtlTransSource (IPS), 743
- Customizing PIM Values at the Interface Level example (24-5), 1125
- cut-and-paste method, installing CA certificates with, 939
- cut-through proxy feature
  - configuring, 211
  - firewall sessions, authentication, 209-214
- CX (ConteXt Security) modules, 268, 335
  - architecture, 273-277
  - Application Inspection Engine, 276
  - Control Plane module, 276-277
  - Data Plane module, 274-275
  - Evening and Reporting module, 275
  - HTTP Inspection Engine module, 276
  - Management Plane module, 276
  - TLS (Transport Layer Security) Decryption Proxy module, 276
  - User Identity module, 275
- component and software updates, 290-292
- configuration database
  - backup, 292-293
- defining context-aware access policies, defining, 324-327
- failover support (PRSM), 283
- hardware modules, 270
- health monitoring, 272
- high availability, 272-273
- integration, 268-273
- interfaces, 270
- licensing, 288-290
- logical architecture, 269-270
- managing with PRSM, 282-293
  - ASA management, 283
  - centralized license management, 283
  - configuring user accounts, 286-288
  - CX failover support, 283
  - Deployment Manager, 283
  - shared objects and policies, 282
  - unified monitoring, 282
  - universal policies, 282
- monitoring, 329-335
  - connection and system events, 331-332
  - dashboard reports, 329-331
  - packet capturing, 332-335
- NG IPS, enabling, 323-324
- objects, 293
  - policy elements
    - application objects, 299-300
    - application-service objects, 303-304
    - configuring header, 294
    - defining, 293-308
    - destination object groups, 305-306
    - file filtering profiles, 306
    - identity objects, 296-297
    - interface roles, 301-302
    - network groups, 295-296
    - NG IPS profiles, 307-308
    - object groups, 293
    - profiles, 294
    - properties, 295
    - secure mobility objects, 300-301
    - service objects, 302-303
    - source object groups, 304-305
    - URL objects, 298
    - user agent objects, 299
    - web reputation profiles, 306-307
- preparing for configuration, 277-282
- software modules, 271
- solutions, 268
- TLS (Transport Layer Security) Decryption, enabling, 316-322
- traffic redirection, configuring, 327-329
- user identity services
  - configuring directory servers, 310-312
  - connecting to AD agent or CDA, 312-313
  - defining user identity discovery policy, 314-316

*enabling, 309-316*  
*tuning authentication settings, 313-314*

## D

### DAP (dynamic access policies)

AAA (authentication, authorization, and accounting) attributes, 1063-1065  
 Access Method tab (ASDM), 1073-1074  
 access policies, defining, 1068-1069  
 Action tab (ASDM), 1068-1069  
 AnyConnect tab (ASDM), 1074  
 architecture, 1061-1062  
 Bookmarks tab (ASDM), 1073  
 clientless remote-access SSL VPNs, 1060-1074  
 configuring, 1062-1074, 1077-1078  
 endpoint attributes, 1066-1068  
 Functions tab (ASDM), 1071  
 Network ACL Filters tab (ASDM), 1069  
 Port Forwarding Lists tab (ASDM), 1072  
 sequence of events, 1062  
 troubleshooting, 1083  
 Webtype ACL Filters tab (ASDM), 1070-1071  
 dap event class, 148  
 dashboard reports, CX (ConteXt Security) modules, 329-331  
 Dashboard section (PRSM interface), 285  
 data interface addressing, failover, 660-662  
 data interfaces  
   clustering, 690-697  
   transparent firewalls, configuring, 605

Data Plane module (CX), 274-275

Datagram Transport Layer Security (DTLS), AnyConnect Secure Mobility Client, configuring, 1108

data-passing interfaces, configuring, 102-106

date, system clock, setting, 116

DCERPC (Distributed Computing Environment Remote Procedure Calls) inspections, 476

deactivating, time-based activation keys, 72

Deactivating a Time-Based Key example (3-5), 72

debug command, 926-928

debug crypto ca command, 973-974

debug crypto ca messages command, 976

debug crypto ca transactions command, 976

debug crypto ikev1 127 command, 973-974

debug dap trace command, 1083-1084

debug dap trace Command example (22-19), 1083-1084

debug disk command, 589

debug eigrp fsm command, 457-460

debug eigrp packets command, 462

debug ftp client command, 589

debug menu dap command, 1079

debug menu dap Command example (22-17), 1079

debug mrrib client command, 1129

debug mrrib io command, 1129

debug mrrib route [group] command, 1129

debug mrrib table command, 1129

debug ospf events command, 439

debug Output to Show IPsec SAs Are Activated example (20-45), 928

debug Output to Show ISAKMP Proposal Is Acceptable example (20-39), 926-927

debug Output to Show Mode-Config Requests example (20-42), 927

debug Output to Show NAT-T Discovery Process example (20-40), 927

debug Output to Show Phase 1 Negotiations Are Completed example (20-43), 928

debug Output to Show Proxy Identities and Phase 2 Proposal Are Accepted example (20-44), 928

debug Output to Show User Is Authenticated example (20-41), 927

debug pim command, 1129

debug pim df-election command, 1129

debug pim group group command, 1129

debug pim interface interface command, 1129

debug pim neighbor command, 1129

debug rip command, 410-411

debug tacacs command, 223-225

debug webvpn svc Command example (23-15), 1117

debugging, L2F table entries, 638

Debugging the L2F Table Entries example (15-23), 638

Debugs Showing IPsec SAs Are Activated example (19-

- 27), 853
- Debugs to Show ISAKMP Proposal Is Acceptable example (19-24), 852
- Debugs to Show Mismatched ISAKMP Policies example (19-28), 854
- Debugs to Show Mismatched Preshared Keys example (19-29), 854
- Debugs to Show Mismatched Proxy Identities example (19-31), 855
- Debugs to Show Phase 1 Negotiations Are Completed example (19-25), 853
- Debugs to Show Proxy Identities and Phase 2 Proposals Are Accepted example (19-26), 853
- Debugs When Incompatible IPsec Transform Set Is Used example (19-30), 855
- decryption, TLS (Transport Layer Security)
  - Decryption, enabling, 316-322
- deep packet inspection, 8
- Default Class and Policy Maps example (13-2), 469
- Default Configuration for Cisco ASA 5505 Appliance example (4-2), 83
- Default Configuration for Cisco ASA 5510 or Later Appliances example (4-1), 82
- Default Information Filtering in EIGRP example (12-40), 453
- default option (port-misuse command), 512
- Default Per-Session PAT Translation Configuration example (16-17), 700
- default post login selection attribute (SSL VPN), 998
- default-inspection-traffic option (match), 471
- Defining a DAP Record example (22-16), 1074
- Defining a Management Access Rule Through CLI example (8-2), 241
- Defining a Static ARP Entry via CLI example (15-13), 615
- Defining a Web-Type ACL example (22-12), 1034
- Defining an ICMP Policy example (8-8), 255
- Defining an L2F Table and Disabling MAC Learning example (15-15), 616
- Defining an NetFlow Export Policy (5-35), 159
- Defining DNS and WINS Servers for Cisco AnyConnect Secure Mobility Clients example (23-8), 1107
- Defining DNS and WINS Servers for IPsec VPN Clients example (20-16), 889
- Defining Dynamic Crypto Map example (20-10), 885
- Defining Pool of Addresses example (20-8), 883
- Defining Pool of Addresses example (23-6), 1103
- Defining Port-Forwarding via CLI example (22-13), 1037
- Defining RADIUS for IPsec Authentication example (20-7), 882
- Defining RADIUS for IPsec Authentication example (22-9), 1003
- Defining RADIUS for IPsec Authentication example (23-3), 1095
- Defining Smart Tunnel via the CLI example (22-14), 1039
- Defining Static Crypto Map example (20-11), 885
- Defining the Config URL example (14-9), 551
- Defining the IGMP Version example (24-4), 1124
- deny option (prefix-list command), 431
- Denying Specific FTP Commands example (13-10), 484
- deployment
  - Active/Standby failover, 680-684
  - AnyConnect client, 1112-1116
  - ASASM (ASA Services Module), 180-183
  - Cisco ASA 5505 model, 33-34
  - client-based remote-access SSL VPNs, 1086-1088
  - clientless remote-access SSL VPNs, 1075-1078
  - IPsec remote-access VPNs, 916-922
  - QoS (Quality of Service), 1155-1162
  - redundant interfaces, 643-644
  - site-to-site IPsec VPNs, 830
    - hub and spoke*, 836-848
    - single site-to-site tunnel configuration*, 831-836
  - transparent firewalls, 616-636
    - MMTFs (multimode transparent firewalls)*, 623-636
    - SMTFs (single-mode transparent firewalls)*, 617-623
  - virtual firewall, 559-585
- Deployment Manager (PRSM), 283
- Description attribute (Add Access Rule dialog box), 236
- Description attribute (Add Management Access Rule), 241
- description command (GTP map), 492

- design, clientless remote-access SSL VPNs, 980-982
- destination address field (IPv6 header), 381
- Destination attribute (Add Access Rule dialog box), 236
- Destination Interface option (Advanced NAT Settings dialog box), 353
- destination object groups (CX), 305-306
- Device Dashboard tab (ASDM), 96-97
- Device endpoint attribute (DAP), 1067
- Device Information section (Device Dashboard tab), 96
- Device Management Feature icon (Configuration screen), 99
- Device Setup Feature icon (Configuration screen), 98
- devices
  - configuration
    - management*, 119-126
    - removing*, 124-126
    - running*, 119-123
    - startup*, 123-124
  - CPUs, monitoring, 165-168
  - monitoring, 165-172
  - remote system management, 126-132
  - setting up names and passwords, 100-102
  - system maintenance, 132-144
    - software installation*, 132-137
  - system monitoring, 144-165
  - troubleshooting issues, 168-172
- DHCP (Dynamic Host Configuration Protocol), 112-113
- DHCPv6, relay, 384-385
- dialog boxes
  - Add AAA Server, 199
  - Add Access Rule, 235-236
  - Add Authentication Rule, 210
  - Add Authorization Rule, 215-216
  - Add Customization Object, 1009
  - Add DNS Inspect, 478
  - Add Identity Certificate, 938
  - Add Management Access Rule, 241-242
  - Add NAT Rule, 366, 368, 370-371
  - Add Network Object, 351-352, 363, 365
  - Add Signature, 756-758
  - Advanced NAT Settings, 352-353, 363-365, 368, 370
  - Edit Interface, 104
  - Edit Network Object, 370
  - Edit Service Policy Rule, 470, 474-476
  - Install Certificate, 937
  - Network Rule, 407
- Differentiated Services Code Point (DSCP), 1138-1141
- digital certificates
  - client-based remote-access SSL VPNs, enrolling, 1090
  - SSL VPNs, enrolling, 988-993
- dir command, 135
- direct call signaling, H.323, 499
- Direction parameter (Add Signature dialog box), 758
- directory servers, configuring, 310-312
- Disable Proxy ARP on Egress Interface option (Advanced NAT Settings dialog box), 352
- disabling
  - DTLS, 1108
  - features, reload requirement, 72
  - IKEv1 processing, outside interface, 124
  - IPS signatures, 791-792
  - message IDs, 118
  - NAT-T for a peer, 827
  - password recovery process, 141-144
  - Sysopt, 886, 1109
- Disabling a Feature with Reload Requirement example (3-6), 72
- Disabling a Message ID example (5-33), 118
- Disabling DTLS example (23-10), 1108
- Disabling IKEv1 Processing on the Outside Interface example (5-7), 124
- Disabling NAT-T for a Peer example (19-14), 827
- Disabling Password Recovery Using Initial Setup example (5-23), 141
- Disabling Sysopt and Configuring ACLs example (20-13), 886
- Disabling Sysopt and Configuring ACLs example (23-11), 1109
- Disabling the Password Recovery Process example (5-22), 141
- Displaying the EIGRP Topology example (12-41), 454
- Displaying the Routing Table via the CLI (12-2), 399
- Distributed Computing Environment Remote Procedure Calls (DCERPC) inspections, 476
- DMZ (demilitarized zones)
  - firewalls, 7
  - networks, static PAT, 364-365
  - web server, dynamic PAT for inside network with static NAT, 363-364
- DNS (Domain Name System)
  - AnyConnect Secure

- Mobility Client, assignment, 1106-1107
  - application inspections, 476-480
  - doctoring, 372-375
  - snooping, BTF (Botnet Traffic Filter), 782-783
  - downloadable ACLs (access control lists), 254
    - configuring, 218-219
  - drop command (GTP map), 492
  - drop option
    - content-length command, 510
    - max-header-length command, 512
    - max-uri-length command, 512
    - port-misuse command, 512
    - request-method command, 514
    - strict-http command, 510
    - transfer-encoding type command, 515
  - dropped packets, monitoring, 171
  - DSCP (Differentiated Services Code Point), 1138-1141
  - dscp option (match), 471
  - DTLS (Datagram Transport Layer Security), AnyConnect Secure Mobility Client, configuring, 1108
  - Dual ISPs feature, 62
  - dynamic access policies (DAP). *See* DAP (dynamic access policies)
  - dynamic blacklist data, BTF (Botnet Traffic Filter), 781-782
  - dynamic NAT, 343-344
  - dynamic PAT, 343-344
    - remote-access VPN clients, 369-371
    - with static NAT for DMZ web server, 363-364
  - dynamic routing over VPN tunnel, OSPF (Open Shortest Path First), 430-433
- ## E
- 
- eap event class, 148
  - eapoudp event class, 148
  - edge protection, ASASM (ASA Services Module), 182-183
  - Edit Interface dialog box, 104
  - Edit Network Object dialog box, 370
  - Edit Service Policy Rule dialog box, 470, 474-476
  - EIGRP (Enhanced Interior Gateway Protocol), 441
    - authentication, 447-448
    - configuring, 441-453
      - route filtering*, 445-447
    - controlling default information, 453
    - enabling, 441-445
    - route redistribution, 450-452
    - route summarization, 448-450
    - split horizon, 450
    - static neighbors, defining, 448
    - troubleshooting, 454-462
  - eigrp event class, 148
  - email event class, 148
  - email logging, 150
  - email servers, defining, 154
  - Enable ISAKMP Captures example (19-32), 856-857
  - Enable Logging attribute (Add Access Rule dialog box), 236
  - Enable Logging attribute (Add Management Access Rule), 242
  - Enable Rule attribute (Add Management Access Rule), 242
  - Enabling Accounting by Using an ACL to Define Interesting Traffic example (7-13), 220
  - Enabling an Interface example (4-10), 104
  - Enabling ARP Inspection example (15-12), 614
  - Enabling Cisco AnyConnect Secure Mobility Client SSL VPN example (23-4), 1098
  - Enabling Command Accounting example (7-14), 222
  - Enabling CTIQBE Inspection example (13-5), 475
  - Enabling DCERPC Inspection example (13-7), 476
  - Enabling DNS Inspection example (13-8), 480
  - Enabling EIGRP via the CLI example (12-33), 444
  - Enabling ESMTP Inspection via the CLI example (13-9), 483
  - Enabling ISAKMP on the Outside Interface example (19-1), 806
  - Enabling ISAKMP on the Outside Interface example (20-1), 872
  - Enabling NAT-T Globally example (20-19), 898
  - Enabling Routed Firewalls example (15-2), 604
  - Enabling Security Contexts example (14-2), 545
  - Enabling SSL VPN on the Outside Interface example (22-10), 1006
  - Enabling SSL VPN on the Outside Interface example (23-5), 1100
  - Enabling Syslog example (5-24), 147
  - Enabling Syslog Timestamps example (5-25), 147
  - Enabling the HTTP Server example (4-8), 93

- Enabling the Local CA example (21-20), 961
  - Enabling Transparent Firewalls example (15-1), 603
  - encoding\_types option (transfer-encoding type command), 515
  - Encryption-3DES-AES feature, 63
  - Encryption-DES feature, 62
  - Endpoint Assessment scans (Host Scan), 1055
    - enabling, 1058
  - endpoint attributes, DAP (dynamic access policies), 1066-1068
  - Enhanced MGCP Inspection example (13-21), 520
  - enrolling digital certificates, SSL VPNs, 988-993
  - enrollment problems, SCEP (Simple Certificate Enrollment Protocol), troubleshooting, 975-976
  - entity MIB notifications, 162
  - environmental traps, 162
  - Errors Due to Incorrect Time and Date Settings During Enrollment example (21-35), 976
  - ESMTP (Extended SMTP), application inspections, 481-483
  - Establishing Serial Console Session to ASA Services Module example (6-3), 177
  - EtherChannel interfaces, configuring, 109-111
  - EtherType ACLs (access control lists), 233
    - configuring, 610-611
  - Evening and Reporting module (CX), 275
  - Event Action parameter (Add Signature dialog box), 758
  - event classes, supported, 148
  - events, IPS (intrusion prevention system)
    - clearing, 778
    - displaying, 776-778
  - Events section (PRSM interface), 285
  - EventStore, IPS (intrusion prevention system), 744
    - clearing, 778
  - Example of Auto NAT (10-2), 355
  - Example of Manual NAT (10-3), 359
  - Example of NAT and ACL Integration in Pre-8.3 Software (10-4), 361
  - Example of NAT and ACL Integration in Version 8.3 and Later Software (10-5), 361-362
  - Example of TCP Intercept (10-1), 346
  - expiration, time-based activation keys, 70-71
  - ext option (request-method command), 514
  - ext\_method option (request-method command), 514
  - extended ACLs (access control lists), 233
  - Extended SMTP (ESMTP), application inspections, 481-483
- ## F
- 
- failover, 62, 652-684
    - Active/Active, 654-656
    - Active/Standby, 654-656
      - deployment scenario, 680-684
    - versus clustering, 685
    - combined licenses, 73-75
    - configuring, 667-678
    - hardware requirements, 656-658
    - health monitoring, 664-666
    - interfaces, 658-664
      - asymmetric routing groups, 662-664
      - data addressing, 660-662
      - link security, 659-660
      - stateful link, 659
    - monitoring, 678-680
    - role transition, 666-667
    - software requirements, 656-658
    - state transition, 666-667
    - stateful, 653-654
    - troubleshooting, 678-680
    - unit roles, 652-653
  - Failover Event Syslog Message example (16-13), 680
  - failover option (system execution space), 534
  - Failover Policy and Timer Configuration example (16-7), 674
  - Failover State Transition History example (16-14), 680
  - Failover Status section (Device Dashboard tab), 97
  - features
    - advanced security, 63-65
      - Advanced Endpoint Assessment, 64
      - AnyConnect for Cisco VPN Phone, 64
      - AnyConnect for Mobile, 64
      - Borner Traffic Filter, 64
      - Cluster, 64-65
      - GTP/GPRS, 64
      - Intercompany Media Engine, 63-64
      - IPS Module, 65
    - basic platform capabilities
      - 10GE I/O, 62
      - Firewall Connections, 61
      - Inside Hosts, 62
      - Maximum Physical Interfaces, 61
      - Maximum VLANs, 61
      - VLAN Trunk Ports, 62
    - licensed, 59-68

- Encryption-3DES-AES*, 63
- Encryption-DES*, 62
- Failover*, 62
- Other VPN Peers*, 63
- Total VPN Peers*, 63
- tiered capacity, 65-66
- AnyConnect Essentials*, 66
- AnyConnect Premium Peers*, 66
- Security Contexts*, 65
- Total UC Proxy Sessions*, 66
- UC Phone Proxy Sessions*, 65-66
- fields, IPv6 headers, 380-381
- file browser attribute (SSL VPN), 998
- File endpoint attribute (DAP), 1067
- file filtering profiles (CX), 306
- file management option (system execution space), 534
- file server entry attribute (SSL VPN), 998
- File Transfer Protocol (FTP). *See* FTP (File Transfer Protocol)
- files, identity certificates, installing from, 938
- filtering
  - packets, 2-3, 229-234
  - PIM (Protocol Independent Multicast) neighbors, 1126-1127
  - route, RIP (Routing Information Protocol), 406-409
  - SSL VPN traffic, 1109
  - traffic, 235-242
    - to-the-box*, 240-242
    - configuring*, 816-817
    - deployment*, 255-260
    - inbound*, 255-260
    - IPv6, 387
    - through-the-box*, 235-240
- Filtering PIM Neighbors
  - example (24-7), 1127
- Filtering SSL VPN Traffic
  - example (23-12), 1109
- Final Chassis Configuration
  - example (6-11), 188
- Firewall Connections
  - feature, 61
- Firewall Feature icon (Configuration screen), 98
- firewall host scans, Host Scan, configuring, 1059
- firewall mode option (system execution space), 534
- firewalls, 2-9
  - Cisco ASA 1000V Cloud Firewall, 26-27
  - deep packet inspection, 8
  - DMZ (demilitarized zones), 7
  - internal segment firewalling, ASASM (ASA Services Module), 181-182
  - multiple-mode, 537
    - packet flow*, 541-544
  - network, 2-7
  - next-generation context-aware, 8
  - Next-Generation Firewall Services, 268
  - personal, 9
  - routed, 591-592
    - versus transparent firewalls*, 593-594
  - sessions
    - authentication*, 209-214
    - troubleshooting*, 225-226
  - single-mode, 537
  - stateful, 267
    - inspection*, 6-7
  - transparent, 591-594, 640
    - architecture*, 593-599
    - configuring*, 602-616
    - deployment scenarios*, 616-636
    - enabling*, 603-604
    - MMTFs (*multimode transparent firewalls*), 597-599
    - monitoring*, 636-637
    - restrictions*, 599-602
    - versus routed firewalls*, 593-594
    - setting up interfaces*, 604-605
    - SMTFs (*single-mode transparent firewalls*), 593-597
    - troubleshooting*, 637-640
- virtual firewall, 531-533, 535, 590
  - architecture*, 533-544
  - configuring security contexts*, 544-559
  - deployment scenarios*, 559-585
  - monitoring security contexts*, 586-588
  - non-shared interfaces*, 559-572
  - packet classification*, 536-541
  - shared interfaces*, 572-585
  - system execution space*, 533
  - troubleshooting*, 588-590
  - user context*, 535-538
- flags, show conn command, 263
- flash logging, 155
- floating connection timeout, static routes, 649
- flow
  - ASASM traffic, managing, 178-180
  - tracing packet, 168-169
- flow director, clustering, 686-687
- flow forwarding, clustering, 686-687
- flow label field (IPv6 header), 381
- flow option (match), 471
- flow owner, clustering, 686



fragmentation policies, site-to-site IPsec VPNs, 829-830

## front panels

- Cisco ASA 5505 model, 30-32
- Cisco ASA 5510 model, 36
- Cisco ASA 5512-X model, 38
- Cisco ASA 5520 model, 36, 41
- Cisco ASA 5540 model, 36
- Cisco ASA 5550 model, 36

FTP (File Transfer Protocol), application inspections, 484-486

FTP logging, 155-156

Full Configuration of the Chicago, London, and Paris ASAs example (19-19), 842-848

Fully Initialized ASA Services Module example (6-2), 176-177

Functions tab (ASDM), 1071

## G

gateway option (route command), 394

ge option (prefix-list command), 431

General Packet Radio Service (GPRS), application inspections, 486-492

Generating RSA Key Pair and Enabling SSH Version 2 example (7-6), 207

Generating the ID Certificate Request example (21-11), 953

Generating the RSA Key Pair example (21-1), 945

global correlation, IPS (intrusion prevention system), 766-768

global threat correlation capabilities, IPS (intrusion prevention system), 14

global unicast addresses, 382

globally enabling security contexts, virtual firewall, 544-546

GPRS (General Packet Radio Service), application inspections, 486-492

GPRS Tunneling Protocol (GTP). *See* GTP (GPRS Tunneling Protocol)

group policies, 876

- client-based remote-access SSL VPNs, configuring, 1090-1094
- SSL VPNs, configuring, 994-998

Group Policy AAA attribute, 1063

Group Policy Definition example (20-3), 876

Group Policy Definition example (23-1), 1092

Group-Policy Definition example (22-5), 996

groups, tunnel, configuring, 997-1000

GTP (GPRS Tunneling Protocol), application inspections, 486-492

GTP Inspection Example (13-12), 491

GTP/GPRS feature, 64

## H

### H.323

- application inspections, 492-499
- components, 493-495
- direct call signaling, 499
- T.38 protocol, 499
- version compatibility, 495-496

H.323 Inspection Commands example (13-13), 498

H.323 Inspection Commands Sent by ASDM example (13-14), 498

HA (high availability), 641

- clustering, 685-731

*configuring*, 706-716

- hardware requirements*, 687-690

*health monitoring*, 697-698

*interfaces*, 690-697

*monitoring*, 717-720

*NAT (Network Address Translation)*, 698-700

*packet flow*, 702-706

*performance*, 700-702

- software requirements*, 687-690

*spanned EtherChannel deployment*, 720-731

*state transition*, 705-706

*troubleshooting*, 717-720

*unit roles*, 685-687

CX (ConteXt Security) modules, 272-273

failover, 652-684

*Active/Active*, 654-656

*Active/Standby*, 654-656, 680-684

*configuring*, 667-678

*hardware requirements*, 656-658

*health monitoring*, 664-666

*interfaces*, 658-664

*monitoring*, 678-680

*role transition*, 666-667

*software requirements*, 656-658

*state transition*, 666-667

*stateful*, 653-654

*troubleshooting*, 678-680

*unit roles*, 652-653

IPS (intrusion prevention system), 739

redundant interfaces, 642-646

static routes

*backup ISP deployment*, 649-652

*configuring with SLA monitor*, 647-648

*floating connection*

- timeout*, 649
- tracking*, 646-652
- ha event class**, 148
- hairpinning IPsec**, 899-901
- hardware modules**
  - CX (ConteXt Security), 270
  - IPS (intrusion prevention system), 735-736
- hardware requirements**
  - clustering, 687-690
  - failover, 656-658
- headers**
  - CX (ConteXt Security)
    - policy elements, configuring, 294
  - IPv6, 380
- health monitoring**
  - clustering, 697-698
  - CX (ConteXt Security)
    - modules, 272
- help FTP command**, 485
- heuristic-based analysis**, 12
- hidden share access attribute (SSL VPN)**, 998
- high availability (HA)**. *See* HA (high availability)
- homepage URL (optional) attribute (SSL VPN)**, 998
- hop limit field (IPv6 header)**, 381
- host chasis, ASASM (ASA Services Module)**
  - integration, 175-176
  - managing, 176-180
- Host Scan**
  - Advanced Endpoint Assessment feature, configuring, 1058-1059
  - antispysware scans, configuring, 1059
  - antivirus host scans, configuring, 1059
  - Basic Host Scan, configuring, 1057-1058
  - clientless remote-access SSL VPNs, 1054-1060
  - configuring, 1056-1060
  - Endpoint Assessment scans, enabling, 1058

- firewall host scans, configuring, 1059
- modules, 1054-1055
- HTTP compression attribute (SSL VPN)**, 998
- HTTP inspection engine**, 507-515
- HTTP Inspection Engine module (CX)**, 276
- HTTP Inspection Using an HTTP Map (13-18)**, 509
- HTTP proxy attribute (SSL VPN)**, 998
- hub and spoke deployment, site-to-site IPsec VPNs**, 836-848

---

## I

- ICMP (Internet Control Message Protocol) packets**
  - inspections, 515-516
  - filtering, 254-255
- ICMP-Type object groups**, 244-245
- identity certificates**
  - installing, 938
  - manually importing, 993
- identity NAT**, 344
  - site-to-site VPN tunnels, 367-369
- identity objects (CX)**, 296-297
- idle timeout, modifying**, 131
- idle timeout attribute (SSL VPN)**, 998
- IDS (intrusion detection systems)**, 9-14
  - anomaly-based analysis, 12-14
  - global threat correlation capabilities, 14
  - heuristic-based analysis, 12
  - pattern matching, 11
  - protocol analysis, 12
  - stateful pattern-matching recognition, 11
- ids event class**, 148
- IGMP (Internet Group Management Protocol)**
  - defining versions, 1123-1124
  - IP multicast routing, 1120
  - query timeout, 1123
  - states, limiting, 1122-1123
- IGMP group, statically assigning**, 1122
- IGMP Query Timeout example (24-3)**, 1123
- IGP (Interior Gateway Protocol)**, 400
- IKE (Internet Key Exchange) protocol**, 16-23
  - IPsec remote-access VPNs
    - IKEv1 configuration*, 862-889
    - IKEv2 configuration*, 889-896
  - site-to-site IPsec VPNs, single site-to-site tunnel configuration, 831-836
- IKEv2 traps**, 162
- ILS (Internet Locator Service), inspections**, 516
- IM (Instant Messenger), inspections**, 517-518
- IM Inspection CLI Configuration example (13-19)**, 518
- im option (port-misuse command)**, 512
- image upgrade**
  - ASDM, 132-133
  - CLI (command-line interface), 133-136
- image upload, ROMMON mode (Read-Only-Memory Monitor mode)**, 136-137
- IME, monitoring IPS**, 793
- Importing the CA Certificate Manually example (21-10)**, 952
- Importing the CA Certificate Manually example (22-1)**, 989
- inbound packet filtering**, 230
- inbound traffic filtering, ACLs (access control lists)**,

- 255-260
- individual mode, clustering, 695-697
- information area, SSL VPNs, 1011
- infrastructure requirements
  - client-based remote-access SSL VPNs, requirements, 1089-1090
  - SSL VPNs, 986-987
- in-interface-name option (mroute command), 1127
- initial setup, 90-100
  - ASDM, 92-100
  - CLI (command-line interface), 90-92
  - configuring interfaces, 102-106
  - configuring system clock, 114-118
  - names and passwords, 100-102
  - parameters and values, 91
- Initial Setup Menu example (4-5), 90-91
- inline mode, IPS (intrusion prevention system), 737-738
- Inside Hosts feature, 62
- inside NAT (Network Address Translation), 338
- inspect icmp command, 515-516
- inspections
  - see also* application inspections
  - ARP, enabling, 613-615
  - deep packet, 8
- Install Certificate dialog box, 937
- installing
  - PKI (Public Key Infrastructure) certificates, 936-957
  - software, 132-137
- Instant Messenger (IM), inspections, 517-518
- Intercompany Media Engine feature, 63-64
- Interface attribute (Add Access Rule dialog box), 235
- Interface attribute (Add Management Access Rule), 241
- interface option (route command), 394
- interface roles (CX), 301-302
- Interface Status section (Device Dashboard tab), 97
- interfaces, 118
  - ACLs (access control lists), transparent firewalls, 608-611
  - CLI (command-line interface), 81, 85-87, 118
  - clientless remote-access SSL VPNs, enabling, 1005-1006
  - configuring, 102-106
  - CX (ConteXt Security) modules, 270
  - EtherChannel, configuring, 109-111
  - failover, 658-664
    - asymmetric routing groups*, 662-664
    - data addressing*, 660-662
    - link security*, 659-660
    - stateful link*, 659
  - management, configuring, 111
  - non-shared, virtual firewall, 559-572
  - PRSM, sections, 285-286
  - redundant, 642-646
    - configuring*, 644-645
    - deploying*, 643-644
    - monitoring*, 645-646
  - shared, virtual firewall, 572-585
  - subinterfaces, configuring, 106-108
  - transparent firewalls, setting up, 604-605
  - VLANs, assigning, 177-178
- Interfaces Feature icon (Monitoring screen), 99
- interfaces option (system execution space), 534
- Interior Gateway Protocol (IGP), 400
- internal segment firewalling, ASASM (ASA Services Module), 181-182
- internal-control interface (CX), 270
- internal-data interface (CX), 270
- Internet access, enabling address translation, 1116
- Internet Control Message Protocol (ICMP) packets, inspections, 515-516
- Internet Key Exchange (IKE) protocol, 16-23
- Internet Locator Service (ILS), inspections, 516
- Intrusion Prevention System (IPS). *See* IPS (intrusion prevention system)
- Invalid Activation Key Rejected example (3-7), 72
- invalid activation keys, 72
- IP Address attribute (Add Network Object dialog box), 351
- IP (Internet Protocol) addresses
  - servers, assignments*, 256
  - transparent firewalls, configuring*, 605-606
- IP DSCP field (QoS), 1138-1141
- ip event class, 148
- IP precedence field (QoS), 1137-1138
- IP (Internet Protocol) routing, 391, 463
  - EIGRP, 441
    - configuring*, 441-453
    - troubleshooting*, 454-462
  - multicast routing, 1119, 1129
    - configuring*, 1120-1127

- enabling multicast routing*, 1121-1124
- IGMP support*, 1120
- PIM (Protocol Independent Multicast)*, *enabling*, 1124-1127
- PIM-SM (Protocol Independent Multicast-Sparse Mode)*, 1120
- troubleshooting*, 1127-1129
- OSPF (Open Shortest Path First), 412-441
  - configuring*, 413-419
  - configuring authentication*, 422-426
  - configuring redistribution*, 426-427
  - dynamic routing over VPN tunnel*, 430-433
  - neighbor command*, 430-433
  - NSSAs, 428-429
  - OSPFv3, 433
  - stub areas*, 428-429
  - troubleshooting*, 433-441
  - Type 3 LSA filtering*, 429-430
  - virtual links*, 419-422
- RIP (Routing Information Protocol), 400-411
  - authentication*, 403-406
  - configuring*, 401-403
  - configuring redistribution*, 409
  - route filtering*, 406-409
  - troubleshooting*, 409-411
- routing tables, displaying, 399-400
- static routes
  - configuring*, 392-400
  - monitoring*, 395-398
- IP Version attribute (Add Network Object dialog box), 351
- ipaa event class, 148
- IPS (intrusion prevention system), 9-14, 733, 786, 787, 799
  - accessing from ASA CLI, 747-748
  - anomaly detection, 763-766
  - anomaly-based analysis, 12-14
  - ASDM, setting up, 752
  - backing up
    - configuration, 776
  - basic management settings, configuring, 748-752
  - BTF (Botnet Traffic Filter), 780-786
  - CIPS (Cisco intrusion Prevention System)
    - accessing CLI*, 747-748
    - configuring on*, 753-768
    - displaying*, 771-772
    - installing*, 744-747
  - license key installation, 752-753
    - troubleshooting*, 1082
    - upgrading*, 772-776
  - CMS event tables, removing false positive events, 794
  - CollaborationApp, 744
  - custom signatures, 755-758
  - displaying statistics, 795-799
  - events
    - clearing*, 778
    - displaying*, 776-778
  - EventStore, 744
  - global correlation, 766-768
  - global threat correlation capabilities, 14
  - HA (high availability), 739
  - hardware modules, 735-736
  - heuristic-based analysis, 12
  - inline mode, 737-738
  - integration, 733-739
  - logical architecture, 735
  - MainApp, 741-743
  - maintaining, 768-778
  - monitoring, tools, 793-794
  - pattern matching, 11
  - preparing for configuration, 744-753
  - process information, displaying, 771-772
  - promiscuous mode, 738-739
  - protocol analysis, 12
  - remote blocking, 758-762
  - risk rating (RR), 789-791
  - SensorApp, 743
  - signatures
    - disabling*, 791-792
    - retiring*, 792-793
    - upgrading*, 772-776
  - software architecture, 739-740
  - software modules, 736
  - stateful pattern-matching recognition, 11
  - traffic redirection, configuring for ASA, 778-780
  - tuning, 787-789
    - tools*, 793-794
  - user accounts, administration, 769-770
- IPS Feature icon (Configuration screen), 98
- IPS Feature icon (Monitoring screen), 100
- IPS Module feature, 65
- IPsec
  - attributes, 20, 804
  - hairpinning, 899-901
  - IPsec remote-access VPNs, 859-862, 929
    - assigning IP addresses*, 882-884
    - bypassing NAT*, 886
    - Cisco IP phone bypass*, 909
    - client firewalling*, 904-907
    - crypto maps, creating*, 884-885
    - deployment*, 916-922
    - defining policies*, 878-879
    - DNS (Domain Name System)*, 888-889
    - group policies*, 875-876

- hardware client network extension mode, 909-910*
  - IKEv1 configuration, 862-889*
  - IKEv2 configuration, 889-896*
  - individual user authentication, 908-909*
  - interactive client authentication, 907-908*
  - IPsec hairpinning, 899-901*
  - L2TP over, 910-916*
  - LEAP bypass, 883-909*
  - monitoring, 922-926*
  - split tunneling, 887-888*
  - traffic filtering, 886*
  - transparent tunneling, 897-899*
  - troubleshooting, 926-928*
  - tunnel and group policies, 874-875*
  - tunnel default gateway, 896-897*
  - user authentication, 879-882*
  - VPN load balancing, 901-904*
  - WINS, 888-889*
  - OSPF (Open Shortest Path First) updates over, 823-824
  - site-to-site IPsec VPNs, 801-802, 857
    - bypassing NAT, 817-818*
    - configuring, 805-822*
    - configuring traffic filtering, 816-817*
    - creating crypto maps, 812-816*
    - creating ISAKMP policy, 807-808*
    - defining IPsec policy, 810-812*
    - deployment scenarios, 830-848*
    - enabling ISAKMP, 806*
    - enabling PFS, 819-820*
    - fragmentation policies, 829-830*
    - management access, 828-829*
    - monitoring, 848-851*
    - NAT-T (NAT Transversal), 826-827*
    - preconfiguration checklist, 802-804*
    - RRI (reverse route injection), 824-826*
    - setting up tunnel groups, 808-810*
    - troubleshooting, 852-857*
    - tunnel default gateway, 827-828*
  - site-to-site tunnels, configuring, 966-971
  - tunnels, transparent firewall restrictions, 599-600
  - traps, 162
  - VPNs (Virtual Private Networks), 16-23
  - IPsec over TCP**
    - Configuration example (20-21), 899**
  - IPsec over UDP**
    - Configuration example (20-20), 899**
  - IPsec pass-through, inspection, 518-519**
  - IPsec Pass-Through Inspection CLI**
    - Configuration example (13-20), 519**
  - IPv6, 379, 390**
    - ACLs (access control lists), configuring, 386-388
    - addresses
      - assigning, 383-384*
      - supported types, 380-382*
      - translation, 389-390*
    - configuring, 382-390
    - DHCP relay, 384-385
    - headers, 380
    - NAT topology, 389
    - optional parameters, 385-386
    - origins, 379-382
    - router advertisement transmission interval, 385-386
    - topology, 386
    - traffic filtering, configuring, 387
  - ISAKMP (Internet Security Association and Key Management Protocol)**
    - attributes, 802
    - enabling, 806, 872
    - policy configuration, 968
  - ISAKMP Policy Configuration example (21-28), 968**
- 
- ## J-L
- Java TAPI (JTAPI), 473
  - JTAPI (Java TAPI), 473
  - Kerberos, Active Directory,
  - L2F Table Aging Time example (15-14), 616**
  - L2F table entries**
    - debugging, 638
    - modifying parameters, transparent firewalls, 615-616
    - transparent firewalls, adding static, 612
  - L2TP over IPsec remote-access VPN, 910-916**
    - configuring, 912-915
    - Windows L2TP over IPsec client configuration, 915-916
  - LACP (Link Aggregation Control Protocol), 644**
  - Latest ASDM Syslog Messages section (Device Dashboard tab), 97**
  - LDAP (Lightweight Directory Access Protocol), 197-198**
  - le option (prefix-list command), 431**
  - levels, security, 145**
  - license aggregation, clustering, 685**

- license keys, CIPS, installing, 752-753
- licensed features, 59-68
  - 10GE I/O, 62
  - advanced security
    - Advanced Endpoint Assessment*, 64
    - AnyConnect for Mobile*, 64
    - AnyConnect for VPN Phone*, 64
    - Botnet Traffic Filter*, 64
    - Cluster*, 64-65
    - GTP/GPRS*, 64
    - Intercompany Media Engine*, 63-64
    - IPS Module*, 65
  - Dual ISPs, 62
  - Encryption-3DES-AES, 63
  - Encryption-DES, 62
  - Failover, 62
  - Firewall Connections, 61
  - Inside Hosts, 62
  - Maximum Physical Interfaces, 61
  - Maximum VLANs, 61
  - Other VPN Peers, 63
  - tiered capacity
    - AnyConnect Essentials*, 66
    - AnyConnect Premium Peers*, 66
    - Security Contexts*, 65
    - UC Phone Proxy Sessions*, 65-66
  - Total VPN Peers, 63
  - VLAN Trunk Ports, 62
- licenses
  - aggregation, rules, 73-74
  - Base, 59-60
  - Basic, 61-63
  - clientless remote-access SSL VPNs, 983-986
  - combined in failover and clustering, 73-75
  - displaying information, 66-68
  - managing, 87-89
    - with activation keys*, 68-73
  - Security Plus, 59-60
  - time-based, aggregated countdown, 75
- licensing, 59, 80
  - clustering, 688-689
  - CX (ConteXt Security) modules, 288-290
  - failover, 658
  - servers, 78-79
  - shared
    - configuring*, 78-80
    - operations*, 76-77
  - shared premium VPN, 75-80
- Lightweight Directory Access Protocol (LDAP). *See* LDAP (Lightweight Directory Access Protocol)
- Limiting IGMP States example (24-2), 1123
- Link Aggregation Control Protocol (LACP), 644
- link security, failover, 659-660
- link-local addresses, 382
- list-name option (prefix-list command), 431
- load balancing
  - Cisco IPsec clients and site-to-site integration, 916-922
  - VPNs (Virtual Private Networks), 901-904
- Loading and Applying Client Profile example (23-14), 1112
- Loading CSD example (22-15), 1047
- local blacklist data, BTF (Botnet Traffic Filter), 781-782
- Local CA (Certificate Authority), 957-966
  - configuring
    - CLI (command-line interface)*, 960-963
    - ASDM (Adaptive Security Device Manager)*, 958-960
  - enrolling users
    - ASDM (Adaptive Security Device Manager)*, 963-965
    - CLI (command-line interface)*, 965-966
- Local CA Certificate Chain example (21-21), 961-962
- Local User Accounts example (20-6), 880
- Local User Accounts example (22-8), 1001
- local user object groups, 244
- log option
  - content-length command, 510
  - max-header-length command, 512
  - max-uri-length command, 512
  - port-misuse command, 512
  - request-method command, 514
  - strict-http command, 510
  - transfer-encoding type command, 515
- Logger (IPS), 742
- logging
  - ASDM (Adaptive Security Device Manager), 150
  - console, 150
  - email, 150
  - flash, 155
  - FTP (File Transfer Protocol), 155-156
  - lists, setting up, 149
  - NSEL (NetFlow Secure Event Logging), 156-160
  - SNMP trap, 151
  - storing logs, 154
  - syslog server, 150
  - system logging, 144-156
    - ASDM logging*, 150
    - buffered logging*, 151-152
    - console*, 150

- email logging*, 150
  - enabling*, 146-149
  - flash logging*, 155
  - FTP logging*, 155-156
  - logging types*, 149
  - SNMP trap logging*, 151
  - storing logs internally and externally*, 154
  - syslog server logging*, 150
  - terminal logging*, 150
  - terminal, 150
  - Logging Feature icon (Monitoring screen), 100
  - Logging in to ASA IPS CLI for the First Time example (17-2), 747-748
  - Logging Interval attribute (Add Management Access Rule), 242
  - logical architecture
    - CX (ConteXt Security) modules, 269-270
    - IPS (intrusion prevention system), 735
  - login screen, PRSM, 283
  - logon area, SSL VPNs, 1010-1011
  - logon page, SSL VPNs, 1006-1008
    - customized, 1016-1018
    - full customization, 1019-1021
  - logout page, SSL VPNs, 1015
  - London's ASA Site-to-Site IPsec Configuration example (21-31), 969-971
  - Lookup Route Table to Locate Egress Interface option (Advanced NAT Settings dialog box), 353
- ## M
- 
- Malware Traffic dashboard (CX), 330
  - Management Access on the Inside Interface example (19-16), 829
  - management interfaces
    - configuring, 111
    - CX (ConteXt Security), 270
  - management IP addresses, transparent firewalls, assigning, 606
  - Management Plane module (CX), 276
  - managing licenses, 87-89
  - Manually Importing the ID Certificate example (21-12), 954
  - Manually Importing the ID Certificate example (22-3), 993
  - Mapped Port option (Advanced NAT Settings dialog box), 353
  - mask option (mroute command), 1127
  - master units, clustering, 685-686
  - match command, 470
  - Matching Specific Traffic Using an ACL example (13-1), 468
  - max option (content-length command), 510
  - max-header-length command, 511-512
  - maximum connect time attribute (SSL VPN), 998
  - Maximum Physical Interfaces feature, 61
  - Maximum VLANs feature, 61
  - max-uri-length command, 512
  - max-value option (prefix-list command), 431
  - mcc command (GTP map), 492
  - MD5 authentication, OSPF (Open Shortest Path First), 424
  - Media Gateway Control Protocol (MGCP), inspections, 519-521
  - Member Class to Context Mapping example (14-17), 559
  - memberOf AAA attribute, 1063
  - message-length command (GTP map), 492
  - metric option (route command), 394
  - MGCP (Media Gateway Control Protocol), inspections, 519-521
  - mini option (content-length command), 510
  - min-value option (prefix-list command), 431
  - Mismatched OSPF Areas example (12-30), 440
  - Mismatched OSPF Authentication Parameters example (12-31), 440
  - MMP Inspection Commands Sent by ASDM example (13-17), 506
  - MMTFs (multimode transparent firewalls), 597-599
    - deploying, 623-636
  - Mobility Proxy feature, 506
  - modes, NAT (Network Address Translation), 349-350
  - Modular Policy Framework (MPF), 468
  - modules
    - CX (ConteXt Security), 268, 335
      - architecture*, 273-277
      - component and software updates*, 290-292
      - configuration database backup*, 292-293
      - defining context-aware access policies*, 324-327
      - failover support (PRSM)*, 283

- hardware modules*, 270
  - health monitoring*, 272
  - high availability*, 272-273
  - integration*, 268-273
  - interfaces*, 270
  - licensing*, 288-290
  - logical architecture*, 269-270
  - managing with PRSM*, 282-293
  - monitoring*, 329-335
  - NG IPS*, 323-324
  - objects*, 293
  - policy elements*, 293-307
  - preparing for configuration*, 277-282
  - software modules*, 271
  - solutions*, 268
  - TLS (Transport Layer Security) decryption*, 316-322
  - traffic redirection*, 327-329
  - user identity services*, 310-316
  - Host Scan, 1054-1055
  - monitoring**
    - ACLs (access control lists), 260-265, 637
    - Active Telnet sessions, 129
    - address translations, 375-377
    - ASASM traffic flow, 179
    - clientless remote-access SSL VPNs, 1078-1081
    - clustering, 697-698, 717-720
    - CX (ConteXt Security) modules, 329-335
    - connection and system events*, 331-332
    - dashboard reports*, 329-331
    - packet capturing*, 332-335
    - failover, 664-666, 678-680
    - IPS (intrusion prevention system), tools, 793-794
    - IPsec remote-access VPNs, 922-926
    - NetFlow exports, 160
    - network access, 260-265
    - QoS (Quality of Service), 1162-1164
    - redundant interfaces, 645-646
    - security contexts, 586-588
    - shared licensing operations, 80
    - site-to-site IPsec VPNs, 848-851
    - TACACS+ transactions, 225
    - transparent firewalls, 636-637
    - Monitoring ACLs example (15-21)**, 637
    - Monitoring and Clearing Active Telnet Sessions example (5-12)**, 129
    - Monitoring and Troubleshooting TACACS+ Transactions with the show aaa-server Command example (7-18)**, 225
    - Monitoring ASASM Traffic Flow from Chassis example (6-6)**, 179
    - Monitoring Cluster Status example (16-24)**, 718
    - Monitoring Failover Status example (16-11)**, 678-679
    - Monitoring NetFlow Exports example (5-36)**, 160
    - Monitoring Redundant Interface Statistics example (16-2)**, 646
    - Monitoring screen (ASDM)**, 99-100
    - More Options drop-down menu**, 236-237
    - MPF (Modular Policy Framework)**, 468
    - mroute command, 1127
    - MSN Messenger, inspections, 517-518
    - multicast routing (IP)**, 1119, 1129
      - configuring, 1120-1127
      - enabling, 1121-1124
      - IGMP support, 1120
      - PIM (Protocol Independent Multicast), enabling, 1124-1127
      - PIM-SM (Protocol Independent Multicast-Sparse Mode), 1120
      - troubleshooting, 1127-1129
    - Multiple Device mode (PRSM)**, 282
    - multiple-mode firewalls**, MMTFs (multimode transparent firewalls), 597-599
      - deployment, 623-636
    - multiple-mode virtual firewalls**, 537
      - packet flow, 541-544
- 
- ## N
- NAC endpoint attribute (DAP)**, 1067
  - nac event class, 148
  - nacpolicy event class, 148
  - nacsettings event class, 148
  - Name attribute (Add Network Object dialog box)**, 351
  - NAT (Network Address Translation)**, 3-4, 337-340, 377
    - ACLs (access control lists), integration, 359-362
    - behavior, 346-350
    - bypassing, 817-818
    - clustering, 698-700
    - configuration
      - automatic*, 351-355
      - manual*, 356-359
      - use cases*, 362-371
    - configuring, 350-371
    - DNS doctoring, 372-375
    - dynamic, 343-344
    - identity, 344
    - inside, 338
    - modes, 349-350



- monitoring translations, 375-377
  - NAT-T (NAT Transversal), 826-827
  - order of operation, 350
  - outside, 339
  - policy, 344
  - security levels, 346-349
  - security protection mechanisms, 345-346
  - static, 341-342
    - configuring*, 611
  - transparent firewalls
    - configuring*, 611-612
    - restrictions*, 600-602
  - traps, 162
  - NAT-T (NAT Transversal), 826-827
    - site-to-site IPsec VPNs, single site-to-site tunnel configuration, 831-836
  - navigation panel, SSL VPNs, 1013
  - negotiations, SSL (Secure Sockets Layer), troubleshooting, 1081
  - neighbor reachable time (IPv6), 385
  - Neighbor Solicitation messages (IPv6), 385
  - neighbors, PIM (Protocol Independent Multicast), filtering, 1126-1127
  - NetBIOS, inspections, 521
  - NetFlow Secure Event Logging (NSEL), 156-160
  - Netmask attribute (Add Network Object dialog box), 351
  - netmask option (route command), 394
  - network access, 265
    - ACLs (access control lists), 243
      - object grouping*, 243-250
    - controlling, 229
    - monitoring control, 260-265
    - packet filtering, 229-234
    - traffic filtering
      - configuring*, 235-242
      - inbound*, 255-260
  - Network ACL Filters tab (ASDM), 1069
  - Network Address Translation (NAT). *See* NAT (Network Address Translation)
  - network firewalls, 2-7
  - network groups (CX), 295-296
  - network option (route command), 394
  - Network Overview dashboard (CX), 330
  - Network Rule dialog box, 407
  - Network Time Protocol (NTP), 116
  - network-based object groups, 244
  - networks. *See* VPNs (Virtual Private Networks)
  - New York ASA Trustpoint Configuration example (21-27), 967
  - next header field (IPv6 header), 381
  - next-generation context-aware firewalls, 8,268
  - NG Intrusion Prevention dashboard (CX), 330
  - NG IPS, enabling, 323-324
  - NG IPS profiles (CX), 307-308
  - no mask-syst-reply Subcommand example (13-11), 486
  - non-shared interfaces, virtual firewall, 559-572
  - NotificationApp (IPS), 743
  - np event class, 148
  - NSEL (NetFlow Secure Event Logging), 156-160
  - NSSA (not-so-stubby areas), OSPF (Open Shortest Path First), 428-429
  - NTP option (system execution space), 534
- 
- ## O
- object group policy element (CX), 293
  - object grouping, ACLs (access control lists), 243-250
  - object policy elements (CX), 293
  - Obtaining the CA Certificate from the CA Server example (21-6), 949
  - Obtaining the ID Certificate from the CA Server example (21-7), 949
  - Operating System endpoint attribute (DAP), 1067
  - operator accounts, IPS (intrusion prevention system), 769
  - optional parameters, IPv6, 385-386
  - Options Available in the show service-policy Command example (25-11), 1162
  - order of operation, NAT (Network Address Translation), 350
  - OSPF (Open Shortest Path First), 412-441
    - ASA configuration, 825
    - authentication, configuring, 422-426
    - configuring, 413-419
    - dynamic routing over VPN tunnel, 430-433
    - enabling, 414-419
    - neighbor command, 430-433
    - NSSAs (not-so-stubby areas), 428-429
    - OSPFv3, 433
    - redistribution, configuring, 426-427
    - static neighbors, 432
    - stub areas, 428-429

troubleshooting, 433-441  
 Type 3 LSA filtering, 429-430  
 updates over IPsec, 823-824  
 virtual links, 419-427  
 OSPF Configuration on the ASA example (19-12), 825  
 ospf event class, 148  
 OSPF MD5 Authentication CLI Commands example (12-18), 424  
 OSPF Static Neighbors example (12-21), 432  
 OSPF Updates over IPsec example (19-9), 824  
 OSPF Virtual Link CLI Configuration example (12-16), 421  
 OSPF Virtual Link MD5 Authentication CLI Commands example (12-19), 426  
 OSPF Virtual Link MD5 Authentication CLI Commands example (12-20), 427  
 OSPFv3, 433  
 Other VPN Peers feature, 63  
 outbound packet filtering, 231  
 out-interface-name option (mroute command), 1127  
 outside NAT (Network Address Translation), 339  
 overlapping subnets, static NAT, 366-367

## P

p2p option (port-misuse command), 512  
 Packet Capturing example (5-43), 170  
 Packet Capturing example (8-13), 264  
 packet classification, QoS (Quality of Service), 1137-1141  
 Packet Dispatcher component (Data Plane), 274  
 packet flow sequence, QoS (Quality of Service), 1136-1137  
 packets  
   capturing, 169-171, 264  
   *CX (ConteXt Security) modules*, 332-335  
   classification, virtual firewall, 536-541  
   deep inspection, 8  
   filtering, 2-3, 229-234  
     *inbound*, 230  
     *outbound*, 231  
   flow  
     *clustering*, 702-706  
     *multiple-mode virtual firewalls*, 541-544  
     *SMTFs (single-mode transparent firewalls)*, 595-597  
   Internet Control Message Protocol (ICMP), inspections, 515-516  
   MMTFs (multimode transparent firewalls), flow, 597-599  
   monitoring dropped, 171  
   tracing flow, 168-169  
   troubleshooting, 168-171  
 parameters  
   initial setup, 91  
   IPv6, optional, 385-386  
 Partial Output of show running-config example (5-2), 122  
 participants, licensing, 79  
 passwords, recovery process, 137-140  
   disabling, 141-144  
 PAT (Port Address Translation), 4-5, 338, 340  
   clustering, 698-700  
   dynamic, 343-344  
     *with static NAT for DMZ web server*, 363-364  
   policy, 344  
   static, 341-342  
 pattern matching  
   IDS (intrusion detection systems), 11  
   IPS (intrusion prevention system), 11  
 payload length field (IPv6 header), 381  
 PBR (policy-based routing)  
   ASASM (ASA Services Module), trusted flow bypass, 183-189  
   configuration, 185-189  
 PD metric (RR), 791  
 Perfect Forward Secrecy (PFS), enabling, 819-820  
 permanent activation keys, 68-71  
 permit command (GTP map), 492  
 permit option (prefix-list command), 431  
 Personal Firewall endpoint attribute (DAP), 1067  
 personal firewalls, 9  
 PFS (Perfect Forward Secrecy), enabling, 819-820  
 Phone Proxy Commands Sent by ASDM example (13-15), 503-504  
 Phone Proxy feature, 500-504  
 PIM (Protocol Independent Multicast)  
   enabling, 1124-1127  
   filtering neighbors, 1126-1127  
   rendezvous points, configuring, 1125-1126  
   static multicast routes, configuring, 1127  
 PIM (Protocol Independent Multicast) sparse mode, PIM-SM (Protocol Independent Multicast-

- Sparse Mode), IP multicast routing, 1120
- PKI (Public Key Infrastructure), 931-932, 977
  - CA (Certificate Authority), 933-935
    - local*, 957-966
  - certificates, 932-933
    - configuring Cisco ASA to accept remote-access IPsec VPN clients*, 971-972
    - configuring IPsec site-to-site tunnels*, 966-971
  - CRLs (*certificate revocation lists*), 935-936
  - installing*, 936-957
  - installing CA certificates with copy-and-paste*, 939
  - installing identity from a file*, 938
  - installing identity using SCEP*, 943-945
  - installing through ASDM*, 936-938
  - installing using CLI*, 945-957
  - installing using SCEP*, 940-943
    - SCEP (*Simple Certificate Enrollment Protocol*), 936
  - troubleshooting, 972-977
- Point-to-Point Tunneling Protocol (PPTP), inspections, 522
- policies
  - context-aware access, defining, 324-327
  - DAP (dynamic access policies), 1060-1074
    - architecture*, 1061-1062
    - configuring*, 1062-1074
    - sequence of events*, 1062
  - group
    - client-based remote-access SSL VPNs*, 1090-1094
    - configuring for SSL VPNs*, 994-998
  - ISAKMP, creating, 807-808
  - tunnel, client-based remote-access SSL VPNs, 1090-1094
- Policies dashboard (CX), 330
- policing traffic, QoS (Quality of Service), 1134-1135, 1149-1150
- policy elements, CX (ConteXt Security) modules
  - application objects, 299-300
  - application-service objects, 303-304
  - configuring header, 294
  - defining, 293-308
  - destination object groups, 305-306
  - file filtering profiles, 306
  - identity objects, 296-297
  - interface roles, 301-302
  - network groups, 295-296
  - NG IPS profiles, 307-308
  - object groups, 293
  - objects, 293
  - profiles, 294
  - properties, 295
  - secure mobility objects, 300-301
  - service objects, 302-303
  - source object groups, 304-305
  - URL objects, 298
  - user agent objects, 299
  - web reputation profiles, 306-307
- Policy endpoint attribute (DAP), 1067
- policy maps, QoS (Quality of Service)
  - applying to interface, 1155
  - configuring, 1153-1154
- policy NAT/PAT, 344
- Policy Table component (Data Plane), 274
- policy-based routing (PBR), ASASM (ASA Services Module), trusted flow bypass, 186
- pools of addresses, defining, 1101-1103
- Port Address Translation (PAT). *See* PAT (Port Address Translation)
- port forwarding, clientless remote-access SSL VPNs, configuring, 1035-1037
- Port Forwarding Lists tab (ASDM), 1072
- port option (match), 471
- port settings, consoles, 84
- portal customization, SSL VPNs, configuring, 1006-1024
- portal customization attribute (SSL VPN), 998
- portal page, SSL VPNs, 1012
  - customized, 1018-1019
- port-forwarding list attribute (SSL VPN), 998
- port-misuse command, 512
- post login setting attribute (SSL VPN), 998
- PPTP (Point-to-Point Tunneling Protocol), inspections, 522
- precedence option (match), 471
- preconfiguration checklist, site-to-site IPsec VPNs, 802-804
- prefix/length option (prefix-list command), 431
- prefix-list command, 430-431
- prerequisites, clientless remote-access SSL VPNs, 982-987
- Presence Federation Proxy feature, 506

- prioritization, traffic, QoS (Quality of Service), 1133, 1148
- priority queuing, QoS (Quality of Service), tuning, 1143-1144, 1152
- Process endpoint attribute (DAP), 1067
- profile policy element (CX), 294
- Promiscuous Delta parameter (Add Signature dialog box), 757
- promiscuous mode, IPS (intrusion prevention system), 738-739
- prompt option (system execution space), 534
- properties, CX policy elements, 295
- Properties Feature icon (Monitoring screen), 100
- protocol analysis, 12
- Protocol option (Advanced NAT Settings dialog box), 353
- protocol-based object groups, 244
- protocols
  - AAA (authentication, authorization, and accounting), 192-198
  - ARP (Address Resolution Protocol), enabling inspection, 613-615
  - DHCP (Dynamic Host Configuration Protocol), 112-113
  - DHCPv6, relay, 384-385
  - EIGRP (Enhanced Interior Gateway Protocol), 441
    - authentication*, 447-448
    - configuring*, 441-453
    - controlling default information*, 453
    - enabling*, 441-445
    - route redistribution*, 450-452
    - route summarization*, 448-450
  - split horizon*, 450
  - static neighbors*, defining, 448
  - troubleshooting*, 454-462
- ICMP (Internet Control Message Protocol), 254-255, 515-516
- IGMP (Internet Group Management Protocol)
  - defining versions*, 1123-1124
  - IP multicast routing*, 1120
  - limiting states*, 1122-1123
  - query timeout*, 1123
- IGP (Interior Gateway Protocol), 400
- IKE (Internet Key Exchange), 16-23
  - IPsec remote-access VPNs*, 862-896
  - site-to-site IPsec VPNs*, *single site-to-site tunnel configuration*, 831-836
- IP (Internet Protocol)
  - addresses*, 256
  - routing*, 391-463, 1119-1127
  - transparent firewalls*, 605-606
- IPsec
  - attributes*, 20, 804
  - hairpinning*, 899-901
  - IPsec remote-access VPNs*, 859-862, 929
  - site-to-site IPsec VPNs*, 801-802, 857
  - site-to-site tunnels*, 966-971
  - VPNs (Virtual Private Networks)*, 16-23
- IPv6, 379, 390
  - ACLs (access control lists)*, 386-388
  - addresses*, 380-390
  - configuring*, 382-390
  - DHCP relay*, 384-385
  - headers*, 380
- NAT topology, 389
  - optional parameters*, 385-386
  - origins*, 379-382
  - router advertisement transmission interval*, 385-386
  - topology*, 386
  - traffic filtering*, 387
- ISAKMP (Internet Security Association and Key Management Protocol)
  - attributes*, 802
  - enabling*, 806, 872
  - policy configuration*, 968
- LACP (Link Aggregation Control Protocol), 644
- LDAP (Lightweight Directory Access Protocol), 197-198
- MGCP (Media Gateway Control Protocol), inspections, 519-521
- OSPF (Open Shortest Path First), 412-441
  - ASA configuration*, 825
  - authentication*, 422-426
  - configuring*, 413-419
  - dynamic routing over VPN tunnel*, 430-433
  - enabling*, 414-419
  - neighbor command*, 430-433
  - NSSAs (not-so-stubby areas)*, 428-429
  - OSPFv3*, 433
  - redistribution*, 426-427
  - static neighbors*, 432
  - stub areas*, 428-429
  - troubleshooting*, 433-441
  - Type 3 LSA filtering*, 429-430
  - updates over IPsec*, 823-824
  - virtual links*, 419-427
- PIM (Protocol Independent Multicast), enabling, 1124-1127

PPTP (Point-to-Point Tunneling Protocol), inspections, 522

RIP (Routing Information Protocol)  
*authentication, 403-406*  
*configuring, 401-403*  
*configuring redistribution, 409*  
*route filtering, 406-409*  
*troubleshooting, 409-411*

SCEP (Simple Certificate Enrollment Protocol), 936  
*enrollment problems, 975-976*  
*installing certificates, 940-943*

SIP (Session Initiation Protocol)  
*inspections, 524-525*  
*timeout, 525*

SNMP (Simple Network Management Protocol)  
*configuring traps, 162-164*  
*inspections, 527-528*  
*system monitoring, 160-165*  
*supported, 466-467*

VPNs (Virtual Private Networks), 14-15

proxies, application, 3

PRSM (Prime Security Manager)  
 interface, sections, 285-286  
 login screen, 283  
 managing CX (ConteXt Security) modules, 282-293  
*ASA management, 283*  
*centralized license management, 283*  
*component and software updates, 290-292*  
*configuration database backup, 292-293*  
*configuring user accounts, 286-288*

*CX failover support, 283*  
*Deployment Manager, 283*  
*licensing, 288-290*  
*Multiple Device mode (PRSM), 282*  
*shared objects and policies, 282*  
*Single Device mode, 282*  
*unified monitoring, 282*  
*universal policies, 282*

**Public Key Infrastructure (PKI).** *See* PKI (Public Key Infrastructure)

## Q

**QoS (Quality of Service), 1131-1132**  
 action rules, applying, 1148  
 architecture, 1136-1142  
 class maps, setting up, 1152-1153  
 configuring, 1142-1155  
*via ASDM, 1143-1151, 1157-1160*  
*via CLI (command-line interface), 1152-1155, 1157-1160*  
 deploying, 1155-1162  
 IP ACLs (access control lists), 1141  
 monitoring, 1162-1164  
 packet classification, 1137-1141  
 packet flow sequence, 1136-1137  
 policy maps  
*applying to interface, 1155*  
*configuring, 1153-1154*  
 priority queuing, tuning, 1143-1144, 1152  
 service policies, defining, 1144  
 traffic

*IP flow, 1141*  
*policing, 1134-1135, 1149-1150*  
*prioritization, 1133, 1148*  
*shaping, 1135-1136, 1150-1151*

Traffic Classification Criteria wizard, 1145-1147

VPN tunnel group, 1141

VPN tunnels, 1142

**Quality of Service (QoS).** *See* QoS (Quality of Service)  
 query timeout, IGMP, 1123

## R

**RADIUS (Remote Authentication Dial In User Service), 191, 194-195**  
 accounting, 220  
 authentication, setting up, 1114-1115

**RADIUS attribute ID, 1063**

**randomization, sequence numbers, 345**

**Rate-Limiting of Tunnel Traffic example (25-7), 1154**

**Read-Only-Memory Monitor mode (ROMMON mode), 87**

**Real Port option (Advanced NAT Settings dialog box), 353**

**Real-Time Streaming Protocol (RTSP), inspections, 523-524**

**Real-time Transport Control Protocol (RTCP), 494-495**

**Real-time Transport Protocol (RTP), 494**

**rear panels**  
 Cisco ASA 5505 model, 32-33  
 Cisco ASA 5510 model, 36  
 Cisco ASA 5512-X model, 38  
 Cisco ASA 5520 model, 41

- recovery process, passwords, 137-140
  - disabling, 141-144
- redesigning address translation, 349-350
- Redistributing Static Routes into EIGRP example (12-39), 452
- redistribution
  - configuring, RIP (Routing Information Protocol), 409
  - EIGRP routes, 450-452
  - OSPF (Open Shortest Path First), configuring, 426-427
- Redundant Interface
  - Configuration example (16-1), 645
- redundant interfaces, 642-646
  - configuring, 644-645
  - deploying, 643-644
  - monitoring, 645-646
- Regex String parameter (Add Signature dialog box), 758
- registry checks, CSD (Cisco Secure Desktop), setting up, 1114
- Registry endpoint attribute (DAP), 1067
- relay, DHCPv6, 384-385
- Release parameter (Add Signature dialog box), 758
- Reloading the Security Appliance example (5-18), 135
- remote access traps, 162
- Remote Access VPN Feature icon (Configuration screen), 98
- remote access VPNs. *See also* IPsec remote-access VPNs
- remote blocking, IPS (intrusion prevention system), 758-762
- Remote Shell (RSH), inspections, 523
- remote system management, 126-132
  - SSH (Secure Shell), 129-132
  - Telnet, 126-129
- remote-access VPN clients
  - Cisco ASA, configuring to accept, 971-972
  - dynamic PAT, 369-371
- Removing a Security Context example (14-14), 554
- Removing All Security Contexts example (14-15), 554
- Removing Existing RSA Key Pair example (21-2), 946
- rendezvous points, PIM (Protocol Independent Multicast), configuring, 1125-1126
- request option (max-header-length command), 512
- request-method command, 513-514
- request-queue command (GTP map), 492
- requirements, CSD (Cisco Secure Desktop), 1044-1045
- reset option
  - content-length command, 510
  - max-header-length command, 512
  - max-uri-length command, 512
  - port-misuse command, 512
  - request-method command, 514
  - strict-http command, 510
  - transfer-encoding type command, 515
- Resetting Hit-Count Counters with clear access-list counters example (8-11), 261
- Resource Allocation for a Member Class example (14-16), 557
- resource management, virtual firewall, 555-559
- resource management option (system execution space), 534
- resource traps, 162
- response option (max-header-length command), 512
- restrict access to VLAN attribute (SSL VPN), 998
- restrictions, transparent firewalls, 599-602
- retiring IPS signatures, 792-793
- retr FTP command, 485
- reverse route injection (RRI), site-to-site IPsec VPNs, 824-826
- Reverting to Single-Mode Firewall example (14-4), 546
- rfc option (request-method command), 514
- rfc\_method option (request-method command), 514
- RIP (Routing Information Protocol), 400-411
  - authentication, 403-406
  - configuring, 401-403
  - configuring redistribution, 409
  - route filtering, 406-409
  - troubleshooting, 409-411
- RIP Authentication Commands Sent to the Cisco ASA example (12-5), 406
- RIP CLI Commands example (12-3), 403
- rip event class, 148
- risk rating (RR), IPS (intrusion prevention system), 789-791
- rm event class, 148
- rnfr FTP command, 485
- rnto FTP command, 485
- role transition, failover, 666-667
- ROMMON mode (Read-

- Only-Memory Monitor mode), 87
- route command, 394-395
- route filtering, EIGRP, configuring, 445-447
- Route Map Using a Standard ACL example (8-6), 251
- route summarization, EIGRP, 448-450
- routed firewalls, 591-592
  - versus transparent firewalls, 593-594
- router advertisement transmission interval, IPv6, 385-386
- routes
  - redistribution, EIGRP, 450-452
  - static
    - backup ISP deployment*, 649-652
    - configuring with SLA monitor*, 647-648
    - floating connection time-out*, 649
    - tracking*, 652
  - transparent firewalls, setting up, 606-607
- routing
  - IP (Internet Protocol), 391
    - configuring static routes*, 392-400
    - displaying routing tables*, 399-400
    - monitoring static routes*, 395-398
  - OSPF (*Open Shortest Path First*), 412-441
  - RIP (*Routing Information Protocol*), 400-411
  - IP multicast, 1119, 1120-1127, 1129
    - enabling*, 1121-1124
    - enabling PIM*, 1124-1127
    - IGMP support*, 1120
    - PIM-SM (Protocol Independent Multicast Sparse Mode)*, 1120
    - troubleshooting*, 1127-1129
  - PBR (policy-based routing), ASASM (ASA Services Module), 183-189
  - PUT IP ROUTING UNDER HERE, 463
  - Routing Feature icon (Monitoring screen), 100
  - Routing Information Protocol (RIP). *See* RIP (Routing Information Protocol)
  - Routing Table After Application of Route Filtering Rules example (12-7), 408
  - Routing Table on Internal Router example (19-13), 826
  - Routing Table on the ASA example (19-11), 825
  - routing tables, displaying, 399-400
  - RR (risk rating), IPS (intrusion prevention system), 789-791
  - RRI (reverse route injection), site-to-site IPsec VPNs, 824-826
    - single site-to-site tunnel configuration, 831-836
  - RSA SecurID (SDI), 196-197
  - RSA Security Analytics, 794
  - RSH (Remote Shell), inspections, 523
  - RTCP (Real-time Transport Control Protocol), 494-495
    - inspections, 523-524
  - RTP (Real-time Transport Protocol), 494
  - rtp option (match), 471
- S**
- Sample CX Redirection Policy example (9-3), 329
- Sample IPS Redirection Policy example (17-7), 780
- SCCP (Simple Client Control Protocol), inspections, 525-527
- SCEP (Simple Certificate Enrollment Protocol), PKI (Public Key Infrastructure), 936
  - enrollment problems, 975-976
  - certificates, installing, 940-943
- SCEP Required AAA attribute, 1063
- SCP file transfer protocol, 132
- Secure Desktop (CSD), 1043
- Secure Desktop Manager (CSD), 1043
- secure mobility objects (CX), 300-301
- Secure Shell (SSH), remote system management, 129-132
- SecureMeInc.org, 592, 617-618
- SecurID (SDI), 196-197
- security, 1, 28
  - AAA (authentication, authorization, and accounting)
    - protocols*, 192-198
    - services*, 192-198
  - accounting
    - configuring*, 219-222
    - TACACS+ (Terminal Access Controller Access Control System Plus)*, 221-222
  - algorithms, support, 129
  - AnyConnect Secure Mobility, 25-26
  - ASDM (Adaptive Security Device Manager)
    - AAA (authentication, authorization, and accounting) test utility*, 226-227
    - Access Method tab*,

- 1073-1074
- accessing, 94-97
- Action tab, 1068-1069
- AnyConnect tab, 1074
- ASA CX Status tab, 97
- Bookmarks tab, 1073
- configuration, 98-99, 257-259
- connections, 208-209
- Content Security tab, 97
- Device Dashboard tab, 96-97
- enabling RIP in, 401
- Firewall Dashboard tab, 97
- Functions tab, 1071
- image upgrade, 133-136
- initial setup, 92-100
- Intrusion Prevention tab, 97
- Local CA (Certificate Authority), 958-960, 963-965
- logging, 150
- monitoring IPS, 793
- Monitoring screen, 99-100
- Network ACL Filters tab, 1069
- PKI (Public Key Infrastructure) certificates, 936-938
- Port Forwarding Lists tab, 1072
- QoS (Quality of Service), 1143-1151, 1157-1160
- setting up for IPS management, 752
- uploading, 92-93
- Webtype ACL Filters tab, 1070-1071
- authentication
  - ASDM connections, 208-209
  - configuring, 204-209
  - configuring of administrative sessions, 204-209
  - configuring OSPF, 422-426
  - customizing, 214-215
  - EIGRP, 447-448
  - RADIUS (Remote Authentication Dial In User Service), 194-195
  - RIP (Routing Information Protocol), 403-406
  - SecurID (SDI), 196-197
  - serial console connections, 207-208
  - service support, 192
  - SSH (Secure Shell) connections, 206-207
  - Telnet connections, 204-206
  - timeouts, 214
- authorization
  - commands, 217-218
  - configuring, 215-219
  - service support, 193
- cloud computing, 26-27
- CX (ConteXt Security) modules, 268
  - architecture, 273-277
  - hardware modules, 270
  - high availability, 272-273
  - managing with PRSM, 282-293
  - preparing for configuration, 277-282
  - software modules, 271
  - solutions, 268
- firewalls, 2-9
  - deep packet inspection, 8
  - DMZ (demilitarized zones), 7
  - next-generation context-aware, 8
  - personal, 9
- IDS (intrusion detection systems), 9-14
- IPS (intrusion prevention system), 9-14, 733, 786, 787, 799
  - accessing CIPS from ASA CLI, 747-748
  - anomaly detection, 763-766
  - anomaly-based analysis, 12-14
  - ASDM, setting up, 752
  - backing up
    - configuration, 776
  - basic management settings, 748-752
  - BTf (Botnet Traffic Filter), 780-786
  - CIPS, 744-776
  - CMS event tables, 794
  - CollaborationApp, 744
  - configuring basic management settings, 748-752
  - configuring CIPS on, 753-768
  - configuring traffic redirection, 778-780
  - custom signatures, 755-758
  - disabling signatures, 791-792
  - events, 776-778
  - EventStore, 744
  - global correlation, 766-768
  - global threat correlation capabilities, 14
  - HA (high availability), 739
  - hardware modules, 735-736
  - heuristic-based analysis, 12
  - inline mode, 737-738
  - installing CIPS license key, 752-753
  - installing CIPS system software, 744-747
  - integration, 733
  - logical architecture, 735
  - MainApp, 741-743
  - maintaining, 768-778
  - monitoring, 793-794
  - pattern matching, 11
  - preparing for configuration, 744-753



- process information, displaying*, 771-772
- promiscuous mode*, 738-739
- remote blocking*, 758-762
- risk rating (RR)*, 789-791
- SensorApp*, 743
- setting up ASDM for*, 752
- signatures*, 772-776, 791-793
- software architecture*, 739-740
- software modules*, 736
- stateful pattern-matching recognition*, 11
- traffic redirection*, 778-780
- tuning*, 787-789, 793-794
- user account administration*, 769-770
- link, failover, 659-660
- PKI (Public Key Infrastructure), 931-932, 977
  - CA (Certificate Authority), 933-935
  - certificates, 932-933, 936
  - configuring Cisco ASA to accept remote-access IPsec VPN clients, 971-972
  - configuring IPsec site-to-site tunnels, 966-971
  - installing certificates, 936-957
  - Local CA (Certificate Authority), 957-966
  - troubleshooting, 972-977
- PRSM (Prime Security Manager)
  - interface, sections, 285-286
  - login screen, 283
  - managing CX (ConteXt Security) modules, 282-293
- QoS (Quality of Service), 1131-1132
  - architecture, 1136-1142
  - configuring, 1142-1155
  - deploying, 1155-1162
  - monitoring, 1162-1164
  - types, 1133-1136
- routed firewalls, 591-592
  - versus transparent firewalls, 593-594
- SSL VPNs, authentication, 987-1004
- SSPs (Security Services Processors), 47
- transparent firewalls, 591-594, 640
  - architecture, 593-599
  - configuring, 602-616
  - deployment scenarios, 616-636
  - enabling, 603-604
  - MMTFs (multimode transparent firewalls), 597-599
  - monitoring, 636-637
  - restrictions, 599-602
  - versus routed firewalls, 593-594
  - setting up interfaces, 604-605
  - SMTFs (single-mode transparent firewalls), 593-597
  - troubleshooting, 637-640
- virtual firewall, 531-533, 590
  - admin context, 535
  - architecture, 533-544
  - configuring security contexts, 544-559
  - deployment scenarios, 559-585
  - monitoring security contexts, 586-588
  - non-shared interfaces, 559-572
  - packet classification, 536-541
  - shared interfaces, 572-585
  - system execution space, 533
  - troubleshooting, 588-590
  - user context, 535-538
  - virtualization, 26-27
  - VPNs (Virtual Private Networks), 14-25
- security appliances, supported subinterfaces, 107
- Security Context Creation Failure
  - example (14-26), 588
- security contexts
  - site-to-site IPsec VPNs, hub and spoke deployment, 836-848
  - virtual firewall
    - configuring, 544-559
    - enabling globally, 544-546
    - managing, 554
    - monitoring, 586-588
  - VLANs, 538
- Security Contexts
  - feature, 65
- Security Group attribute (Add Access Rule dialog box), 236
- Security Group attribute (Add Management Access Rule), 241
- security levels
  - descriptions, 145
  - NAT (Network Address Translation), 346-349
- security object groups, 244
- Security Plus license, 59-60
- security protection mechanisms, address translation, 345-346
- Security Services Processors (SSPs), 47
- selective application inspection, 469-473
- Selective Output of show running-config example (5-3), 122
- SensorApp, IPS (intrusion prevention system), 743
- seq seq-value option (prefix-list command), 431
- sequence numbers, random-

- ization, 345
- sequence of events, DAP (dynamic access policies), 1062
- serial console connections, authentication, 207-208
- server-based object groups, configuring, 247-248
- servers
  - authentication, defining, 198-204
  - email, defining, 154
  - IP address assignments, 256
  - licensing, 78-79
  - shared licenses, 76
  - syslog
    - defining*, 153-154
    - logging*, 150
- service accounts, IPS (intrusion prevention system), 770
- Service attribute (Add Access Rule dialog box), 236
- Service attribute (Add Management Access Rule), 241
- service objects (CX), 302-303
- service policies, QoS (Quality of Service), defining, 1144
- Service Ports parameter (Add Signature dialog box), 758
- service-based object group, 244
- services
  - AAA (authentication, authorization, and accounting), 192-198
  - DHCP, 112-113
- session event class, 148
- Session Initiation Protocol (SIP)
  - inspections, 524-525
  - timeout, 525
- Setting the Boot Parameter
  - example (5-16), 135
- Setting the System Clock and Time Zone example (4-17), 114-116
- Setting Up a Default Gateway Toward the Inside Interface (15-8), 607
- Setting Up a Default Gateway Toward the Management Interface example (15-7), 607
- Setting Up a Logging List example (5-26), 149
- Setting Up a Logging List for Multiple Destinations example (5-27), 152
- Setting Up an Admin Context example (14-11), 552
- Setting Up Optional IPv6 Parameters example (11-3), 386
- Setting Up SNMP Version 3 (5-37), 164
- Setting Up Syslog Servers example (5-29), 154
- Setting Up TFTP Parameters example (5-20), 136
- Setting Up the Hostname, Domain Name, and Passwords example (4-9), 102
- SFR metric (RR), 790-791
- shaping traffic, QoS (Quality of Service), 1135-1136, 1150-1151
- shared interfaces
  - forwarding with, 542-544
  - forwarding without, 541-542
  - virtual firewall, 572-585
- Shared License Server Statistics example (3-10), 80
- shared licensing
  - configuring, 78-80
  - monitoring operation, 80
  - operations, 76-77
- shared objects and policies (PRSM), 282
- Shared Premium licensing, SSL VPNs, 985
- shared premium VPN licensing, 75-80
- show aaa-server command, 225
- show aaa-server protocol command, 202-203
- show access-list outside access\_in command, 261
- show admin-context command, 586
- show asp drop command, 171, 587-588
- show block command, 167
- show clock command, 974-975
- show cluster command, 717
- show cluster Command Options example (16-23), 717
- show conn command, 262, 637
  - flags, 263
- show conn state ctiqbe command, 475
- show context command, 586, 587
- show cpu usage command, 165
- show cpu usage context command, 587
- show crypto accelerator statistics Command Output example (20-37), 924-925
- show crypto ca certificates command, 974-975
- show crypto ca crls command, 957
- show crypto ca server certificate command, 962-963
- show crypto ca server command, 962-963
- show crypto ca server user-db username user1 command, 966

- show crypto ikev1 sa detail command, 924
- show crypto ikev1 sa detail Command Output example (20-35), 924
- show crypto ipsec sa command, 849-850, 924
- show crypto ipsec sa Command Output example (20-36), 924
- show crypto isakmp sa detail command, 848-849
- show crypto protocol statistics ikev1/ipsec commands, 925-926
- show eigrp events command, 455, 461-462
- show eigrp interfaces command, 456
- show eigrp neighbors command, 454
- show eigrp traffic command, 456
- show firewall command, 636
- show igmp groups command, 1128
- show igmp interface command, 1128
- show igmp traffic command, 1128
- show interface command, 105-106
- show local-host command, 376
- show logging command, 152
- show memory command, 166
- show mfib command, 1128
- show mode command, 586
- show mroute command, 1128
- show mroute summary command, 1128
- show nat detail command, 377
- show ntp status command, 118
- show ospf [process-id] command, 434
- show ospf command, 419
- show ospf database command, 437
- show ospf interface command, 434-435
- show ospf neighbor command, 435
- show ospf neighbor detail command, 435
- show ospf virtual-links command, 422, 440-441
- show pim df command, 1128
- show pim group-map command, 1128
- show pim interface command, 1128
- show pim join-prune statistic command, 1128
- show pim neighbor command, 1128
- show pim range-list command, 1128
- show pim topology command, 1128
- show pim traffic command, 1128
- show pim tunnel command, 1128
- show priority-queue statistics command, 1163-1164
- show route command, 403, 410
- show route inside command, 418, 445
- show running-config command output, 120-121
  - from interface configuration, 123*
  - partial output, 122
  - selective output, 122
- show service-policy command, 472-473, 1162
- show service-policy interface outside command, 1163
- show snmp-server statistics command, 165
- show startup-config command, output, 123-124
- show statistics analysis-engine command, 795-796
- show statistics analysis-engine Command Output example (18-2), 795-796
- show statistics authentication command, 796
- show statistics authentication Command Output example (18-3), 796
- show statistics command, 795
- show statistics Command Options example (18-1), 795
- show statistics event-server Command, 796
- show statistics event-server Command Output example (18-4), 796
- show statistics event-store Command, 797
- show statistics event-store Command Output example (18-5), 797
- show statistics host Command, 797-798
- show statistics host Command Output example (18-6), 797-798
- show statistics logger command, 798-799
- show statistics logger Command Output example (18-7), 799
- show uauth command, 226
- show version command, 136
- show vpn-sessiondb detail command, 922-923
- show vpn-sessiondb detail Command Output example (20-33), 922-923
- show vpn-sessiondb remote command, 923
- show vpn-sessiondb remote Command Output example (20-34), 923
- show vpn-sessiondb summary command, 851
- show vpn-sessiondb summary Command Output

- example (19-23), 851
- show xlate command, 375
- Sig Fidelity Rating parameter (Add Signature dialog box), 757
- Signature ID parameter (Add Signature dialog box), 757
- Signature Name parameter (Add Signature dialog box), 758
- signatures, IPS (intrusion prevention system)
  - custom, 755-758
  - disabling, 791-792
  - retiring, 792-793
  - upgrading, 772-776
- Simple Certificate Enrollment Protocol (SCEP), PKI (Public Key Infrastructure), 936
- Simple Client Control Protocol (SCCP), inspections, 525-527
- Simple Network Management Protocol (SNMP). *See* SNMP (Simple Network Management Protocol)
- simultaneous logins attribute (SSL VPN), 998
- Single Device mode (PRSM), 282
- Single Sign-on Definition via the CLI example (22-11), 1031
- single sign-on server attribute (SSL VPN), 998
- single site-to-site tunnel configuration, site-to-site IPsec VPNs, 831-836
- single-mode firewalls
  - reverting to, 546
  - SMTFs (single-mode transparent firewalls), 593-597
    - deploying, 617-623
- single-mode virtual firewalls, 537
- SIP (Session Initiation Protocol)
  - inspections, 524-525
  - timeout, 525
- SIP Timeout Example example (13-22), 525
- site FTP command, 485
- site-local addresses, 382
- site-to-site IPsec VPNs, 801-802, 857
  - configuring, 805-822
    - alternative methods, 820-822
  - crypto maps, creating, 812-816
  - deployment, 830
    - hub and spoke, 836-848
    - single site-to-site tunnel configuration, 831-836
  - fragmentation policies, 829-830
  - IPsec, defining policy, 810-812
- ISAKMP
  - creating policy, 807-808
  - enabling, 806
  - management access, 828-829
  - monitoring, 848-851
- NAT (Network Address Translation), bypassing, 817-818
- NAT-T (NAT Transversal), 826-827
- OSPF (Open Shortest Path First) updates over IPsec, 823-824
- PFS (Perfect Forward Secrecy), enabling, 819-820
- preconfiguration checklist, 802-804
- RRI (reverse route injection), 824-826
- traffic filtering, configuring, 816-817
- troubleshooting, 852-857
- tunnel default gateway, 827-828
- tunnel groups, setting up, 808-810
- Site-to-Site VPN Feature icon (Configuration screen), 98
- site-to-site VPN tunnels, identity NAT, 367-369
- sizes, buffers, 166
- Skinny (SCCP), inspections, 525-527
- SLA monitor, static routes, configuring, 647-648
- slave units, clustering, 685-686
- smart tunnel attribute (SSL VPN), 998
- smart tunnels, clientless remote-access SSL VPNs, configuring, 1037-1040
- SMTFs (single-mode transparent firewalls), 593-597
  - deploying, SMTFs (single-mode transparent firewalls), 617-623
- SNMP (Simple Network Management Protocol)
  - configuring traps, 162-164
  - inspections, 527-528
  - system monitoring, 160-165
- snmp event class, 148
- SNMP Inspection example (13-23), 527-528
- SNMP trap logging, 151
- software, installing, 132-137
- software architecture, IPS (intrusion prevention system), 739-740
- software modules, IPS (intrusion prevention system), 736
- software modules (CX), 271
- software requirements
  - client-based remote-access SSL VPNs, 1088-1089
  - clustering, 687-690
  - failover, 656-658
  - SSL VPNs, 986-987
- source address field (IPv6 header), 381
- Source attribute (Add Access Rule dialog box), 235
- Source attribute (Add

- Management Access Rule), 241
- Source Information option (Advanced NAT Settings dialog box), 353
- source object groups (CX), 304-305
- Source Service attribute (Add Management Access Rule), 242
- spanned EtherChannel deployment, clustering, 720-731
- spanned EtherChannel mode, clustering, 693-695
- Specifying the ASDM Location example (4-7), 93
- split horizon, EIGRP, 450
- Split Tunnel Configuration example (20-15), 888
- split tunneling, AnyConnect Secure Mobility Client, 1103-1106
- Splunk, 794
- SQL\*Net, inspections, 528
- src option (mroute command), 1127
- SSH (Secure Shell)
  - connections, authentication, 206-207
  - monitoring sessions, 131
  - remote system management, 129-132
- SSL (Secure Sockets Layer)
  - clientless remote-access SSL VPNs, prerequisites, 982-987
  - negotiations, troubleshooting, 1081
- SSL (Secure Sockets Layer) VPNs, 979-980, 987-988
  - AnyConnect SSL VPNs configuring, 1115-1116
  - troubleshooting, 1116-1118
  - attributes, configurable, 998
  - authentication, configuring, 987-1004
  - client-based remote-access SSL VPNs, 1085, 1118
  - AnyConnect secure mobility client configuration*, 1096-1112
  - configuring, 1090-1095, 1090-1094
  - deploying, 1086-1088
  - enrolling digital certificates, 1090
  - prerequisites, 1088-1090
  - tunnel policies, 1090-1094
  - user authentication, 1094-1095
- clientless remote-access SSL VPNs, 1084
  - configuring, 1004-1041
  - configuring application access, 1034-1040
  - configuring bookmarks, 1024-1031
  - configuring client-server plug-ins, 1040-1041
  - configuring smart tunnels, 1037-1040
  - configuring web-type ACLs, 1031-1034
  - CSD (Cisco Secure Desktop), 1041-1053
  - DAP (dynamic access policies), 1060-1074
  - deploying, 1075-1078
  - enabling on interfaces, 1005-1006
  - Host Scan, 1054-1060
  - monitoring, 1078-1081
  - troubleshooting, 1081-1084
- content area, 1014
- copyright area, 1011
- design considerations, 980-982
- digital certificates, enrolling, 988-993
- group policies, configuring, 994-998
- information area, 1011
- logon area, 1010-1011
- logon page, 1006-1008
  - customized, 1016-1018
  - full customization, 1019-1021
- logout page, 1015
- navigation panel, 1013
- portal customization, configuring, 1006-1024
- portal page, 1012
  - customized, 1018-1019
- servers, 1004
- title area, 1008-1010
- title panel, 1012
- Toolbar screen, 1013
- tunnel groups, configuring, 997-1000
- tunnel policies, configuring, 994-995
- user portal page, full customization, 1021-1024
- SSL-based VPNs (Virtual Private Networks), 23-25
- ssl event class, 148
- SSPs (Security Services Processors), 47
- standard ACLs (access control lists), 233, 250-251
- standard SNMP traps, 162
- Standby MAC and IP Address Configuration example (16-4), 661
- startup configuration, 123-124
- state transition
  - clustering, 705-706
  - failover, 666-667
- stateful connection redundancy, clustering, 685
- stateful failover, 653-654
- stateful firewalls, 267
- stateful inspection firewalls, 6-7
- stateful links, failover, 659
- stateful pattern-matching recognition
  - IDS (intrusion detection systems), 11
  - IPS (intrusion prevention system), 11

- Stateful Session Creation Failure on Standby ASA example (16-12), 679
- static address translation, 5-6
- static IP routes, configuring, 392-400
- Static L2F Entry entry (15-11), 612
- static L2F table entries, transparent firewalls, adding, 612
- static multicast routes, PIM (Protocol Independent Multicast), configuring, 1127
- static NAT, 341-342
  - configuring, 611
  - with dynamic PAT for DMZ web server, 363-364
  - overlapping subnets, 366-367
- static neighbors, EIGRP, defining, 448
- static PAT, 341-342
  - web servers on DMZ networks, 364-365
- static routes
  - backup ISP deployment, 649-652
  - configuring with SLA monitor, 647-648
  - floating connection timeout, 649
  - tracking, 646-652
- Static Routing Commands Sent by ASDM (12-1), 398
- Statically Assigning an IGMP Group example (24-1), 1122
- statistics, IPS (intrusion prevention system), displaying, 795-799
- status LEDs
  - Cisco ASA 5505 model, 32
  - Cisco ASA 5510 model, 36
  - Cisco ASA 5512-X model, 38-39
  - Cisco ASA 5520 model, 36
  - Cisco ASA 5540 model, 36
  - Cisco ASA 5550 model, 36
  - Cisco ASA 5585-X Series model, 48
- stor FTP command, 485
- storage key attribute (SSL VPN), 998
- storage objects attribute (SSL VPN), 998
- storing, logs internally and externally, 154
- stou FTP command, 485
- strict-http command, 510
- stub areas, OSPF (Open Shortest Path First), 428-429
- subinterfaces, configuring, 106-108
- SubSignature ID parameter (Add Signature dialog box), 757
- Successfully Activated Permanent Key example (3-2), 71
- Sun Remote Procedure Call (RPC), inspections, 522-523
- supported address types, IPv6, 380-382
- Supported Traffic Classification Options example (13-3), 470
- svc event class, 148
- SVC Logging example (23-16), 1118
- Switching to System Execution Space example (14-5), 548
- sys event class, 148
- syslog
  - enabling timestamps, 147
  - messages, 273, 640
  - traps, 162
- syslog message ID tuning, 156
- Syslog Message with a Fail-Close Policy and ASA CX Down example (9-1), 273
- syslog servers
  - defining, 153-154
  - logging, 150
- system clock
  - automatic clock adjustment, 116-118
  - configuring, 114-118
  - date, setting, 116
  - manual adjustment, 114-116
  - time zone, setting, 114-115
- System Context Configuration with Failover Groups example (16-8), 676-677
- system events, CX (ConteXt Security) modules, 331-332
- system execution space, virtual firewall, 533
  - adding user contexts, 549
  - configuring, 562-563
  - switching to, 548
- system logging, 144-156
  - ASDM logging, 150
  - buffered logging, 151-152
  - console, 150
  - email logging, 150
  - enabling, 146-149
  - flash logging, 155
  - FTP logging, 155-156
  - logging types, 149
  - SNMP trap logging, 151
  - storing logs internally and externally, 154
  - syslog server logging, 150
  - terminal logging, 150
- system maintenance, 119, 132-144
  - software installation, 132-137
- system monitoring, 144-165
  - NSEL (NetFlow Secure Event Logging), 156-160
  - SNMP (Simple Network Management Protocol), 160-165
  - system logging, 144-156

System Resources Status section (Device Dashboard tab), 97

## T

T.38 protocol, 499

TACACS+ (Terminal Access Controller Access Control System Plus), 191, 195-196

accounting, 221-222

TAPI (Telephony Application Programming Interface), 473

TCP connection processing, cluster packet flow, 702-703

TCP Intercept, 346

TCP Proxy component (Data Plane), 275

Telephony Application Programming Interface (TAPI), 473

Telnet

connections, authentication, 204-206

remote system management, 126-132

Terminal Access Controller Access Control System Plus (TACACS+). *See* TACACS+ (Terminal Access Controller Access Control System Plus)

terminal logging, 150

test aaa-server authentication command, 227

test aaa-server authentication Command example (7-20), 227

TFTP (Trivial File Transfer Protocol), inspections, 528

through-the-box traffic filtering, 235-240

tiered capacity features, 65-66

AnyConnect Essentials, 66

AnyConnect Premium Peers, 66

Security Contexts, 65

tiered capacity, Security Contexts, 65

UC Phone Proxy Sessions, 65-66

time, system clock, setting, 116

time and date mismatch, PKI (Public Key Infrastructure), troubleshooting, 972-975

Time Range attribute (Add Management Access Rule), 242

time zone, system clock, setting, 114-115

time-based ACLs (access control lists), 251-253

Time-Based Activation Key Aggregation (3-4), 71

time-based activation keys, 68-70, 71

aggregation, 71

deactivating, 72

expiration, 70-71

time-based license count-down, aggregated, 75

timeout

floating connection, static routes, 649

SIP (Session Initiation Protocol), 525

timeout command (GTP map), 492

timeouts, authentication, 214

Time-Range Configuration example (8-7), 253

timestamps, syslog, enabling, 147

title area, SSL VPNs, 1008-1010

title panel, SSL VPNs, 1012

TLS (Transport Layer Security) Decryption configuring, 318-320

CX (ConteXt Security) mod-

ules, enabling, 316-322  
defining decryption policy, 320-322

TLS (Transport Layer Security) Decryption Proxy module, 276

TLS Proxy Commands Sent by ASDM example (13-16), 506

TLS Proxy feature, 505-506

Toolbar screen, SSL VPNs, 1013

topologies

EIGRP, displaying, 454

IPv6, 386

NAT, 389

Total UC Proxy Sessions feature, 66

Total VPN Peers feature, 63

tracing, packet flow, 168-169

Tracing Packet Through the CLI example (5-42), 169

track number option (route command), 394

tracking static routes, 652

traffic

filtering

*AnyConnect Secure Mobility Client*, 1108

*to-the-box*, 240-242

*configuring*, 816-817

*deployment*, 255-260

*inbound*, 255-260

IPv6, 387

*through-the-box*, 235-240

matching specific, ACLs (access control lists), 468

QoS (Quality of Service), 1131-1132

*architecture*, 1136-1142

*configuring*, 1142-1155

*monitoring*, 1162-1164

*policing*, 1134-1135,

1149-1150

- prioritization*, 1133, 1148
  - shaping*, 1135-1136
- redirection
  - CX (ConteXt Security) modules*, 327-329
  - IPS (intrusion prevention system)*, 778-780
- shaping, 1154
- QoS (Quality of Service), 1150-1151
- traffic class field (IPv6 header), 381
- Traffic Classification Criteria wizard, QoS (Quality of Service), 1145-1147
- traffic flow, ASASM (ASA Services Module), managing, 178-180
- Traffic Prioritization for the VoIP Traffic example (25-6), 1154
- traffic selection, BTF (Botnet Traffic Filter), 783-786
- Traffic Shaping and Hierarchical Traffic Priority example (25-8), 1154
- Traffic Status section (Device Dashboard tab), 97
- transaction size attribute (SSL VPN), 998
- transfer-encoding type command, 515
- Transform Set Configuration example (19-4), 811
- Transform Set Configuration example (20-5), 879
- Translate DNS Replies for Rule option (Advanced NAT Settings dialog box), 352
- translation, IPv6 addresses, 389-390
- Translation Addr attribute (Add Network Object dialog box), 351
- transparent firewalls, 591-594, 640
  - architecture, 593-599
  - configuring, 602-616
    - adding static L2F table entries*, 612
    - enabling ARP inspection*, 613-615
    - guidelines*, 602-603
    - interface ACLs*, 608-611
    - IP addresses*, 605-606
    - modifying L2F table parameters*, 615-616
    - NAT (Network Address Translation)*, 611-612
    - routes*, 606-607
    - setting up interfaces*, 604-605
  - deploying, 616-617
    - MMTFs (multimode transparent firewalls)*, 623-636
    - SMTFs (single-mode transparent firewalls)*, 617-623
  - enabling, 603-604
  - MMTFs (multimode transparent firewalls), 597-599
  - monitoring, 636-637
  - restrictions, 599-602
  - versus routed firewalls, 593-594
  - SMTFs (single-mode transparent firewalls), 593-597
    - deploying*, 617-623
  - troubleshooting, 637-640
- transparent mode option (system execution space), 534
- transparent tunneling, IPsec remote-access VPNs, 897-899
- traps, SNMP (Simple Network Management Protocol), configuring, 162-164
- Trend Micro Content Security (CSC-SSM) Feature icon (Configuration screen), 99
- Trend Micro Content Security Feature icon
  - (Monitoring screen), 100
- Trivial File Transfer Protocol (TFTP), inspections, 528
- troubleshooting
  - administrative connections, 222-227
  - AnyConnect SSL VPNs, 1116-1118
  - clientless remote-access SSL VPNs, 1081-1084
  - clustering, 717-720
  - CPUs, 172
  - devices, 168-172
  - EIGRP, 454-462
  - failover, 678-680
  - firewall sessions, 225-226
  - IP multicast routing, 1127-1129
  - IPsec remote-access VPNs, 926-928
  - OSPF (Open Shortest Path First), 433-441
  - packets, 168-171
  - PKI (Public Key Infrastructure), 972-977
  - RIP (Routing Information Protocol), 409-411
  - site-to-site IPsec VPNs, 852-857
  - transparent firewalls, 637-640
  - virtual firewall, 588-590
- trusted flow bypass, ASASM (ASA Services Module), PBR (policy-based routing), 183-189
- tuning IPS (intrusion prevention system), 787-789
  - tools, 793-794
- tunnel default gateway
  - IPsec remote-access VPNs, 896-897
  - site-to-site IPsec VPNs, 827-828
- Tunnel Default Gateway Configuration example (19-15), 828
- Tunnel Default Gateway Configuration example (20-



- 18), 897
  - Tunnel Group Configuration example (21-30), 968
  - Tunnel Group Definition example (19-3), 810
  - Tunnel Group Definition example (20-4), 877
  - Tunnel Group Definition example (22-6), 999
  - Tunnel Group Definition example (23-2), 1093
  - Tunnel Group URL Definition example (22-7), 1000
  - tunnel groups
    - configuration, 968
    - definition, 810, 877, 999, 1093
    - setting up, 808-810
    - SSL VPNs, configuring, 997-1000
  - tunnel policies, client-based remote-access SSL VPNs, 1090-1094
  - tunneled option (route command), 394
  - tunnel-group option (match), 471
  - tunneling, AnyConnect Secure Mobility Client, features, 1103-1109
  - tunneling option (port-misuse command), 512
  - tunneling protocols attribute (SSL VPN), 998
  - tunnel-limit command (GTP map), 492
  - tunnels
    - smart, configuring, 1037-1040
    - VPN (Virtual Private Network), QoS (Quality of Service), 1142
  - TVR metric (RR), 790
  - Type 3 LSA filtering, OSPF (Open Shortest Path First), 429-430
  - Type attribute (Add Network Object dialog box), 351
- ## U
- 
- UC (Unified Communications) advanced support, application inspections, 499-506
  - UC Phone Proxy Sessions feature, 65-66
  - UDP connection processing, cluster packet flow, 702-703
  - Unified Communications (UC) advanced support, application inspections, 499-506
  - unified monitoring (PRSM), 282
  - Uninstalling AnyConnect Client After Session Disconnects example (23-9), 1108
  - unit roles
    - clustering, 685-687
    - failover, 652-653
  - universal policies (PRSM), 282
  - Universal Resource Identifier (URI), 512
  - updates, CX (ConteXt Security) modules, 290-292
  - upgrading CIPS system software, 772-776
  - uploading ASDM, 92-93
  - Uploading the ASDM Image to the Local Flash example (4-6), 92-93
  - URI (Universal Resource Identifier), 512
  - URL entry attribute (SSL VPN), 998
  - URL objects (CX), 298
  - user accounts
    - configuring, PRSM, 286-288
    - IPS (intrusion prevention system), administration, 769-770
  - user agent objects (CX), 299
  - User attribute (Add Access Rule dialog box), 236
  - User attribute (Add Management Access Rule), 241
  - user authentication, client-based remote-access SSL VPNs, 1094-1095
  - User Comments parameter (Add Signature dialog box), 758
  - user context, virtual firewall, 535-538
    - adding, 549
    - configuring, 553-554
  - User Devices dashboard (CX), 330
  - User Identity module (CX), 275
  - user identity services, CX (ConteXt Security) modules
    - configuring directory servers, 310-312
    - connecting to AD agent or CDA, 312-313
    - defining user identity discovery policy, 314-316
    - enabling, 309-316
    - tuning authentication settings, 313-314
  - user portal page, SSL VPNs, full customization, 1021-1024
  - user storage location attribute (SSL VPN), 998
  - Username AAA attribute, 1063
  - Users dashboard (CX), 330
  - Using the CLI to Configure Authentication for Telnet Connections example (7-5), 206
- ## V
- 
- values, initial setup, 91
  - Verifying Chassis Is Redirecting Traffic to the ASA Services Module example (6-12), 189

- Verifying Firewalls Mode example (15-3), 604
- Verifying the Admin Context example (14-12), 553
- Verifying the Maximum Number of Security Contexts example (14-27), 588
- Verifying the Number of Security Contexts example (14-1), 536
- Verifying the TFTP Parameters example (5-21), 137
- Verifying Virtual Firewall Mode example (14-3), 546
- Verifying VPN Client Use of IPsec over TCP example (20-22), 899
- version field (IPv6 header), 381
- viewer accounts, IPS (intrusion prevention system), 769
- Viewing RSA Key Pair Information example (21-3), 946
- virtual firewall, 531-533, 590
  - admin context, 535
    - configuring*, 552-553, 563-568
  - architecture, 533-544
  - configuration URL, specifying, 550-551
  - deployment scenarios, 559-585
  - interfaces, configuring, 549-550
  - multiple-mode, 537
    - packet flow*, 541-544
  - non-shared interfaces, 559-572
  - packet classification, 536-541
  - resource management, 555-559
  - security contexts
    - configuring*, 544-559
    - enabling globally*, 544-546
    - managing*, 554
    - monitoring*, 586-588
  - shared interfaces, 572-585
  - single-mode, 537
    - reverting to*, 546
  - system execution space, 533
    - adding user contexts*, 549
    - configuration*, 562-563
    - setting up*, 547-549
    - switching to*, 548
  - troubleshooting, 588-590
  - user context, 535-538
    - configuring*, 553-554
- virtual links, OSPF (Open Shortest Path First), 419-422
- virtualization, 26-27
- VLAN Assignment to ASA Services Modules example (6-4), 178
- VLAN Trunk Ports feature, 62
- VLANs (virtual LANs)
  - supported security contexts, 538
  - interfaces, assigning, 177-178
- vm event class, 148
- vpdn event class, 148
- vpn event class, 148
- VPN Feature icon (Monitoring screen), 100
- VPN Filters example (20-14), 886
- VPN Flex licenses, SSL VPNs, 985-986
- VPN Load-Balancing Configuration with Encryption example (20-24), 904
- VPN Sessions section (Device Dashboard tab), 97
- vpnc event class, 148
- vpnfo event class, 148
- vpnlb event class, 148
- VPNs (Virtual Private Networks), 14-25
  - AnyConnect SSL VPNs,
    - configuring*, 1115-1116
    - troubleshooting, 1116-1118
  - client-based remote-access SSL VPNs, 1085, 1118
    - AnyConnect secure mobility client configuration*, 1096-1112
    - configuring*, 1090-1095, 1090-1094
    - deploying*, 1086-1088
    - enrolling digital certificates*, 1090
    - prerequisites*, 1088-1090
    - tunnel policies*, 1090-1094
    - user authentication*, 1094-1095
  - clientless remote-access SSL VPNs, 1084
    - configuring application access*, 1034-1040
    - configuring bookmarks*, 1024-1031
    - configuring smart tunnels*, 1037-1040
  - CSD (Cisco Secure Desktop), 1041-1053
  - DAP (dynamic access policies), 1060-1074
  - deploying*, 1075-1078
  - enabling on interfaces*, 1005-1006
  - Host Scan*, 1054-1060
  - monitoring*, 1078-1081
  - prerequisites*, 982-987
  - troubleshooting*, 1081-1084
- IPsec, 16-23
- IPsec remote-access VPNs, 859-862, 929
  - Cisco IP phone bypass*, 909
  - client firewalling*, 904-907
  - deployment*, 916-922
  - hardware client network extension mode*, 909-910

- IKEv1 configuration*, 862-889
- IKEv2 configuration*, 889-896
- individual user authentication*, 908-909
- interactive client authentication*, 907-908
- IPsec hairpinning*, 899-901
- L2TP over*, 910-916
- LEAP bypass*, 883-909
- monitoring*, 922-926
- transparent tunneling*, 897-899
- troubleshooting*, 926-928
- tunnel default gateway*, 896-897
- VPN load balancing*, 901-904
- site-to-site IPsec VPNs, 801-802, 857
  - bypassing NAT*, 817-818
  - configuring*, 805-822
  - configuring traffic filtering*, 816-817
  - creating crypto maps*, 812-816
  - creating ISAKMP policy*, 807-808
  - defining IPsec policy*, 810-812
  - deployment scenarios*, 830-848
  - enabling ISAKMP*, 806
  - enabling PFS*, 819-820
  - fragmentation policies*, 829-830
  - management access*, 828-829
  - monitoring*, 848-851
  - NAT-T (NAT Transversal)*, 826-827
  - OSPF (Open Shortest Path First) updates over IPsec*, 823-824
  - preconfiguration checklist*, 802-804
  - RRI (reverse route injection)*, 824-826
  - setting up tunnel groups*, 808-810
  - troubleshooting*, 852-857
  - tunnel default gateway*, 827-828
- SSL VPNs, 979-980, 987-988
  - clientless remote-access SSL VPNs*, 1004-1041
  - configurable attributes*, 998
  - configuring authentication*, 987-1004
  - configuring portal customization*, 1006-1024
  - configuring tunnel groups*, 997-1000
  - content area*, 1014
  - copyright area*, 1011
  - customized logon page*, 1016-1018
  - customized portal page*, 1018-1019
  - design considerations*, 980-982
  - full customization of logon page*, 1019-1021
  - full customization of user portal page*, 1021-1024
  - information area*, 1011
  - logon area*, 1010-1011
  - logon page*, 1006-1008
  - logout page*, 1015
  - navigation panel*, 1013
  - portal page*, 1012
  - title area*, 1008-1010
  - title panel*, 1012
  - Toolbar screen*, 1013
- SSL-based, 23-25
- tunnels, QoS (Quality of Service), 1142

## W-Z

---

- WAAS (Wide Area Application Services), inspections, 528
- web ACL attribute (SSL VPN), 998
- Web Categories dashboard (CX), 330
- Web Destinations dashboard (CX), 330
- web reputation profiles (CX), 306-307
- webfo event class, 148
- Webtype ACL Filters tab (ASDM), 1070-1071
- Webtype ACLs, 234
  - clientless remote-access SSL VPNs, configuring, 1031-1034
- webvpn event class, 148
- Wide Area Application Services (WAAS), inspections, 528
- Windows NTLM, 197
- WINS, AnyConnect Secure Mobility Client, assignment, 1106-1107
- WLR metric (RR),
- Yahoo! IM (Instant Messenger), inspections, 517
- Zero Downtime upgrade, clustering, 688-689