CCNA Security 640-554

KEITH BARKER, CCIE® No. 6783
SCOTT MORRIS, CCIE® No. 4713
KEVIN WALLACE, CCIE® No. 7945
MICHAEL WATKINS

ciscopress.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 about 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. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Corporate and Government Sales

Cisco Press offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales. For more information, please contact: U.S. Corporate and Government Sales 1-800-382-3419 corpsales@pearsontechgroup.com

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

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.

Publisher: Paul Boger
Manager, Global Certification: Erik Ullanderson
Associate Publisher: Dave Dusthimer
Business Operation Manager, Cisco Press: Anand Sundaram
Executive Editor: Brett Bartow
Technical Editors: Brandon Anastasoff and David Burns
Managing Editor: Sandra Schroeder
Development Editor: Andrew Cupp
Senior Project Editor: Tonya Simpson
Editorial Assistant: Vanessa Evans
Indexer: Heather McNeill
Copy Editor: Keith Cline
Book Designer: Gary Adair
Compositor: Mark Shirar
About the Authors

Keith Barker, CCIE No. 6783 (R&S and Security), is a 27-year veteran of the networking industry. He currently works as a network engineer and trainer for Copper River IT. His past experience includes EDS, Blue Cross, Paramount Pictures, and KnowledgeNet, and he has delivered CCIE-level training over the past several years. As part of the original set of Cisco VIPs for the Cisco Learning Network, he continues to give back to the community in many ways. He is CISSP and CCSI certified, loves to teach, and keeps many of his video tutorials at http://www.youtube.com/keith6783. He can be reached at Keith.Barker@CopperRiverIT.com or by visiting http://www.CopperRiverIT.com.

Scott Morris, CCIE No. 4713 (R&S, ISP/Dial, Security, and Service Provider), has more than 25 years in the industry. He also has CCDE and myriad other certifications, including nine expert-level certifications spread over four major vendors. Having traveled the world consulting for various enterprise and service provider companies, Scott currently works at Copper River IT as the chief technologist. He, too, has delivered CCIE-level training and technology training for Cisco Systems and other technology vendors. Having spent a “past life” (early career) as a photojournalist, he brings interesting points of view from entering the IT industry from the ground up. As part of the original set of Cisco VIPs for the Cisco Learning Network, he continues to give back to the community in many ways. He can be reached at smorris@CopperRiverIT.com or by visiting http://www.CopperRiverIT.com.

About the Contributing Authors

Kevin Wallace, CCIE No. 7945, is a certified Cisco instructor holding multiple Cisco certifications, including CCSP, CCVP, CCNP, and CCDP. With Cisco experience dating back to 1989, Kevin has been a network design specialist for the Walt Disney World Resort, a senior technical instructor for SkillSoft/Thomson NETg/KnowledgeNet, and a network manager for Eastern Kentucky University. Kevin holds a bachelor of science degree in electrical engineering from the University of Kentucky. Kevin has also authored or co-authored multiple books for Cisco Press, including CCNP TSHOOT 642-832 Cert Kit, CCNP TSHOOT 642-832 Official Certification Guide, CCNP ROUTE 642-902 Cert Kit, and CCNP Routing and Switching Official Certification Library, all of which target the current CCNP certification.

Michael Watkins, CCNA/CCNP/CCVP/CCSP, is a full-time senior technical instructor with SkillSoft. With 12 years of network management, training, and consulting experience, Michael has worked with organizations such as Kraft Foods, Johnson and Johnson, Raytheon, and the United States Air Force to help them implement and learn the latest network technologies. In addition to holding over more than 20 industry certifications in the areas of networking and programming technologies, Michael holds a bachelor of arts degree from Wabash College.
About the Technical Editors

Brandon Anastasoff has been a systems engineer with Cisco Systems since October 2007, when he moved from a lead network architect role in a major newspaper-publishing firm. He has spent more than 20 years in the industry, focusing on security for the past 10 and obtaining certifications inside and outside of Cisco, with his CISSP, CCSP, and most recently, the Security CCIE. After studying in the United Kingdom, Brandon took a year off in Saudi Arabia to see what a real job would be like before proceeding to college, but found the lure of an income too irresistible and never went back for the degree. Brandon had to make a choice early in his career to either follow the art of computer animation or the up-and-coming PC networking boom, and he has never regretted the decision to enter networking. He moved from early versions of Windows and Macintosh operating systems through Novell’s NetWare, and then moved more into the infrastructure side, focusing mostly on Cisco LAN/WAN equipment. After Y2K, the focus became more security oriented, and Brandon became familiar with virus and Trojan analysis and forensic investigations. Today, Brandon is glad to be where he is and enjoys talking about security whenever the opportunity presents itself.

David Burns has in-depth knowledge of routing and switching technologies, network security, and mobility. He is currently a systems engineering manager for Cisco covering various U.S. service provider accounts. In July 2008, Dave joined Cisco as a lead systems engineer in a number of areas, including Femtocell, Datacenter, MTSO, and Security Architectures working for a U.S.-based SP Mobility account. He came to Cisco from a large U.S.-based cable company where he was a senior network and security design engineer. Dave held various roles before joining Cisco during his 10-plus years in the industry, working in SP operations, SP engineering, SP architecture, enterprise IT, and U.S. military intelligence communications engineering. He holds various sales and industry/Cisco technical certifications, including the CISSP, CCSP, CCDP, and two associate-level certifications. Dave recently passed the CCIE Security Written, and is currently preparing for the CCIE Security Lab. Dave is a big advocate of knowledge transfer and sharing and has a passion for network technologies, especially as related to network security. Dave has been a speaker at Cisco Live on topics such as Femtocell (IP mobility) and IPS (security). Dave earned his Bachelor of Science degree in telecommunications engineering technology from Southern Polytechnic State University, Georgia, where he currently serves as a member of the Industry Advisory Board for the Computer & Electrical Engineering Technology School.
Dedications

From Keith:
To my parents for bringing me into this world, to my children for perpetuating this world, and to my wonderful wife, Jennifer, for making my current world a better place. I love you, Jennifer.

From Scott:
The variety of inspirations and muses that affect a person's life vary over time. Every one of them affects us in different ways to help shape or drive us to where we are today. I certainly enjoy all the influences that have helped to shape (or warp) me to where I currently am. To my friend and co-author Keith, for convincing me that this was a good idea and a lot of fun to do (and gently “reminding” me of that along the way). To my dear friend Amy (who is smarter than I am) for continuing to tell me that I need to get my CCIE Voice taken care of and prodding me along now and then, motivating me to be something more than what I am currently. To my dear friend Angela, who enjoys keeping me both sane and humble by poking holes in my plans and helping me make things even better while keeping my sense of humor intact. And to my two little girls, who help keep my perspective on the world both healthy and a little off-kilter.

Acknowledgments

We want to thank many people for helping us put this book together.

The Cisco Press team: Brett Bartow, the executive editor, was the catalyst for this project, coordinating the team and ensuring that sufficient resources were available for the completion of the book. Andrew Cupp, the development editor, has been invaluable in producing a high-quality manuscript. His great suggestions and keen eye caught some technical errors and really improved the presentation of the book. We would also like to thank Tonya Simpson and the production team for their excellent work in shepherding this book through the editorial process and nipping at our heels where necessary. Many thanks go to Keith Cline for going the extra mile during the copy edit.

The technical reviewers: We want to thank the technical reviewers of this book, Brandon Anastasoff and David Burns, for their thorough, detailed review and very valuable input.

Our families: Of course, this book would not have been possible without the constant understanding and patience of our families. They have lived through the long days and nights it took to complete this project, and have always been there to poke, prod, motivate, and inspire us. We thank you all.

Each other: Last, but not least, this book is a product of work by two co-workers and colleagues, who have worked together at three different companies over the past 5 years and still manage to stay friends, which made it even more of a pleasure to complete.
## Contents at a Glance

**Introduction**  xxv

**Part I   Fundamentals of Network Security   3**
- Chapter 1   Networking Security Concepts  5
- Chapter 2   Understanding Security Policies Using a Lifecycle Approach  23
- Chapter 3   Building a Security Strategy  37

**Part II   Protecting the Network Infrastructure   47**
- Chapter 4   Network Foundation Protection  49
- Chapter 5   Using Cisco Configuration Professional to Protect the Network Infrastructure  63
- Chapter 6   Securing the Management Plane on Cisco IOS Devices  91
- Chapter 7   Implementing AAA Using IOS and the ACS Server  137
- Chapter 8   Securing Layer 2 Technologies  175
- Chapter 9   Securing the Data Plane in IPv6  199

**Part III   Mitigating and Controlling Threats   219**
- Chapter 10   Planning a Threat Control Strategy  221
- Chapter 11   Using Access Control Lists for Threat Mitigation  235
- Chapter 12   Understanding Firewall Fundamentals  267
- Chapter 13   Implementing Cisco IOS Zone-Based Firewalls  291
- Chapter 14   Configuring Basic Firewall Policies on Cisco ASA  327
- Chapter 15   Cisco IPS/IDS Fundamentals  371
- Chapter 16   Implementing IOS-Based IPS  389

**Part IV   Using VPNs for Secure Connectivity   421**
- Chapter 17   Fundamentals of VPN Technology  423
- Chapter 18   Fundamentals of the Public Key Infrastructure  441
- Chapter 19   Fundamentals of IP Security  465
Chapter 20  Implementing IPsec Site-to-Site VPNs  495
Chapter 21  Implementing SSL VPNs Using Cisco ASA  529
Chapter 22  Final Preparation  559

Part V  Appendixes  565
A  Answers to the “Do I Know This Already?” Quizzes  567
B  CCNA Security 640-554 (IINSv2) Exam Updates  573
    Glossary  577
    Index  587

CD-Only Appendixes
C  Memory Tables  3
D  Memory Tables Answer Key  33
# Contents

Introduction xxv

## Part I  Fundamentals of Network Security 3

### Chapter 1  Networking Security Concepts 5

*“Do I Know This Already?” Quiz 5*

**Foundation Topics 8**

Understanding Network and Information Security Basics 8

Network Security Objectives 8

Confidentiality, Integrity, and Availability 8

Cost-Benefit Analysis of Security 9

Classifying Assets 10

Classifying Vulnerabilities 11

Classifying Countermeasures 12

What Do We Do with the Risk? 12

Recognizing Current Network Threats 13

Potential Attackers 13

Attack Methods 14

Attack Vectors 15

Man-in-the-Middle Attacks 15

Other Miscellaneous Attack Methods 16

Applying Fundamental Security Principles to Network Design 17

Guidelines 17

How It All Fits Together 19

**Exam Preparation Tasks 20**

Review All the Key Topics 20

Complete the Tables and Lists from Memory 20

Define Key Terms 20

### Chapter 2  Understanding Security Policies Using a Lifecycle Approach 23

*“Do I Know This Already?” Quiz 23*

**Foundation Topics 25**

Risk Analysis and Management 25

Secure Network Lifecycle 25

Risk Analysis Methods 25

Security Posture Assessment 26

An Approach to Risk Management 27

Regulatory Compliance Affecting Risk 28
### Chapter 5 Using Cisco Configuration Professional to Protect the Network Infrastructure

#### “Do I Know This Already?” Quiz

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introducing Cisco Configuration Professional</td>
<td>65</td>
</tr>
<tr>
<td>Understanding CCP Features and the GUI</td>
<td>65</td>
</tr>
<tr>
<td>Setting Up New Devices</td>
<td>69</td>
</tr>
<tr>
<td>CCP Building Blocks</td>
<td>70</td>
</tr>
<tr>
<td>CCP Audit Features</td>
<td>81</td>
</tr>
<tr>
<td>Exam Preparation Tasks</td>
<td>88</td>
</tr>
</tbody>
</table>

---

#### Command Reference to Check Your Memory

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Menu Bar</td>
<td>66</td>
</tr>
<tr>
<td>The Toolbar</td>
<td>67</td>
</tr>
<tr>
<td>Left Navigation Pane</td>
<td>68</td>
</tr>
<tr>
<td>Content Pane</td>
<td>69</td>
</tr>
<tr>
<td>Status Bar</td>
<td>69</td>
</tr>
<tr>
<td>Communities</td>
<td>70</td>
</tr>
<tr>
<td>Templates</td>
<td>74</td>
</tr>
<tr>
<td>User Profiles</td>
<td>78</td>
</tr>
<tr>
<td>One-Step Lockdown</td>
<td>84</td>
</tr>
<tr>
<td>A Few Highlights</td>
<td>84</td>
</tr>
<tr>
<td>Complete the Tables and Lists from Memory</td>
<td>88</td>
</tr>
<tr>
<td>Define Key Terms</td>
<td>88</td>
</tr>
</tbody>
</table>
Chapter 6  Securing the Management Plane on Cisco IOS Devices  91

“Do I Know This Already?” Quiz  91

Foundation Topics  94

Securing Management Traffic  94

Beyond the Blue Rollover Cable  94
Management Plane Best Practices  95
Password Recommendations  97
Using AAA to Verify Users  97

AAA Components  98

Options for Storing Usernames, Passwords, and Access Rules  98

Authorizing VPN Users  99
Router Access Authentication  100

The AAA Method List  101

Role-Based Access Control  102
Custom Privilege Levels  103

Limiting the Administrator by Assigning a View  103

Encrypted Management Protocols  103
Using Logging Files  104
Understanding NTP  105
Protecting Cisco IOS Files  106

Implement Security Measures to Protect the Management Plane  106

Implementing Strong Passwords  106
User Authentication with AAA  108
Using the CLI to Troubleshoot AAA for Cisco Routers  113

RBAC Privilege Level/Parser View  118
Implementing Parser Views  120

SSH and HTTPS  122
Implementing Logging Features  125

Configuring Syslog Support  125

SNMP Features  128
Configuring NTP  131
Securing the Cisco IOS Image and Configuration Files  133

Exam Preparation Tasks  134
Review All the Key Topics  134
Complete the Tables and Lists from Memory  135
Define Key Terms  135
Command Reference to Check Your Memory  135
Chapter 7  Implementing AAA Using IOS and the ACS Server  137

“Do I Know This Already?” Quiz  137

Foundation Topics  140

Cisco Secure ACS, RADIUS, and TACACS  140

Why Use Cisco ACS?  140
What Platform Does ACS Run On?  141
What Is ISE?  141
Protocols Used Between the ACS and the Router  141
Protocol Choices Between the ACS Server and the Client (the Router)  142

Configuring Routers to Interoperate with an ACS Server  143
Configuring the ACS Server to Interoperate with a Router  154
Verifying and Troubleshooting Router-to-ACS Server Interactions  164

Exam Preparation Tasks  171

Review All the Key Topics  171
Complete the Tables and Lists from Memory  171
Define Key Terms  171
Command Reference to Check Your Memory  172

Chapter 8  Securing Layer 2 Technologies  175

“Do I Know This Already?” Quiz  175

Foundation Topics  178

VLAN and Trunking Fundamentals  178

What Is a VLAN?  178
Trunking with 802.1Q  180
Following the Frame, Step by Step  181
The Native VLAN on a Trunk  181
So, What Do You Want to Be? (Says the Port)  182
Inter-VLAN Routing  182
The Challenge of Using Physical Interfaces Only  182
Using Virtual “Sub” Interfaces  182
Spanning-Tree Fundamentals  183
Loops in Networks Are Usually Bad  184
The Life of a Loop  184
The Solution to the Layer 2 Loop  184
STP Is Wary of New Ports  187
Improving the Time Until Forwarding  187
Common Layer 2 Threats and How to Mitigate Them 188
  Disrupt the Bottom of the Wall, and the Top Is Disrupted, Too 188
Layer 2 Best Practices 189
Do Not Allow Negotiations 190
Layer 2 Security Toolkit 190
Specific Layer 2 Mitigation for CCNA Security 191
  BPDU Guard 191
  Root Guard 192
  Port Security 192
Exam Preparation Tasks 195
  Review All the Key Topics 195
  Complete the Tables and Lists from Memory 195
  Review the Port Security Video Included with This Book 196
  Define Key Terms 196
  Command Reference to Check Your Memory 196

Chapter 9  Securing the Data Plane in IPv6 199
  “Do I Know This Already?” Quiz 199
Foundation Topics 202
  Understanding and Configuring IPv6 202
    Why IPv6? 202
    The Format of an IPv6 Address 203
    Understanding the Shortcuts 205
    Did We Get an Extra Address? 205
    IPv6 Address Types 206
Configuring IPv6 Routing 208
  Moving to IPv6 210
Developing a Security Plan for IPv6 210
  Best Practices Common to Both IPv4 and IPv6 210
  Threats Common to Both IPv4 and IPv6 212
  The Focus on IPv6 Security 213
  New Potential Risks with IPv6 213
  IPv6 Best Practices 214
Exam Preparation Tasks 216
  Review All the Key Topics 216
  Complete the Tables and Lists from Memory 216
  Define Key Terms 217
  Command Reference to Check Your Memory 217
Part III  Mitigating and Controlling Threats 219

Chapter 10  Planning a Threat Control Strategy  221
“Do I Know This Already?” Quiz  221
Foundation Topics  224
Designing Threat Mitigation and Containment  224
   The Opportunity for the Attacker Is Real  224
   Many Potential Risks  224
   The Biggest Risk of All  224
   Where Do We Go from Here?  225
Securing a Network via Hardware/Software/Services  226
   Switches  227
   Routers  228
   ASA Firewall  230
   Other Systems and Services  231
Exam Preparation Tasks  232
Review All the Key Topics  232
Complete the Tables and Lists from Memory  232
Define Key Terms  232

Chapter 11  Using Access Control Lists for Threat Mitigation  235
“Do I Know This Already?” Quiz  235
Foundation Topics  238
Access Control List Fundamentals and Benefits  238
   Access Lists Aren’t Just for Breakfast Anymore  238
   Stopping Malicious Traffic with an Access List  239
   What Can We Protect Against?  240
   The Logic in a Packet-Filtering ACL  241
   Standard and Extended Access Lists  242
   Line Numbers Inside an Access List  243
   Wildcard Masks  244
   Object Groups  244
Implementing IPv4 ACLs as Packet Filters  244
   Putting the Policy in Place  244
   Monitoring the Access Lists  255
   To Log or Not to Log  257
Implementing IPv6 ACLs as Packet Filters  259
Exam Preparation Tasks  263
Review All the Key Topics  263
Chapter 12 Understanding Firewall Fundamentals 267
“Do I Know This Already?” Quiz 267
Foundation Topics 270
Firewall Concepts and Technologies 270
Firewall Technologies 270
Objectives of a Good Firewall 270
Firewall Justifications 271
The Defense-in-Depth Approach 272
Five Basic Firewall Methodologies 273
Static Packet Filtering 274
Application Layer Gateway 275
Stateful Packet Filtering 276
Application Inspection 277
Transparent Firewalls 277
Using Network Address Translation 278
NAT Is About Hiding or Changing the Truth About Source Addresses 278
Inside, Outside, Local, Global 279
Port Address Translation 280
NAT Options 281
Creating and Deploying Firewalls 283
Firewall Technologies 283
Firewall Design Considerations 283
Firewall Access Rules 284
Packet-Filtering Access Rule Structure 285
Firewall Rule Design Guidelines 285
Rule Implementation Consistency 286
Exam Preparation Tasks 288
Review All the Key Topics 288
Complete the Tables and Lists from Memory 288
Define Key Terms 288

Chapter 13 Implementing Cisco IOS Zone-Based Firewalls 291
“Do I Know This Already?” Quiz 291
Foundation Topics 294
Cisco IOS Zone-Based Firewall 294
  How Zone-Based Firewall Operates 294
  Specific Features of Zone-Based Firewalls 294
  Zones and Why We Need Pairs of Them 295
  Putting the Pieces Together 296
  Service Policies 297
  The Self Zone 300
Configuring and Verifying Cisco IOS Zone-Based Firewall 300
  First Things First 301
  Using CCP to Configure the Firewall 301
  Verifying the Firewall 314
  Verifying the Configuration from the Command Line 315
  Implementing NAT in Addition to ZBF 319
  Verifying Whether NAT Is Working 322
Exam Preparation Tasks 324
  Review All the Key Topics 324
  Review the Video Bonus Material 324
  Complete the Tables and Lists from Memory 324
  Define Key Terms 325
  Command Reference to Check Your Memory 325

**Chapter 14 Configuring Basic Firewall Policies on Cisco ASA 327**

“Do I Know This Already?” Quiz 327

Foundation Topics 330
  The ASA Appliance Family and Features 330
    Meet the ASA Family 330
    ASA Features and Services 331
  ASA Firewall Fundamentals 333
    ASA Security Levels 333
    The Default Flow of Traffic 335
    Tools to Manage the ASA 336
    Initial Access 337
    Packet Filtering on the ASA 337
    Implementing a Packet-Filtering ACL 338
    Modular Policy Framework 338
    Where to Apply a Policy 339
  Configuring the ASA 340
    Beginning the Configuration 340
    Getting to the ASDM GUI 345
Chapter 15  Cisco IPS/IDS Fundamentals  371

“Do I Know This Already?” Quiz  371

Foundation Topics  374

IPS Versus IDS  374

What Sensors Do  374

Difference Between IPS and IDS  374

Sensor Platforms  376

True/False Negatives/Positives  376

Positive/Negative Terminology  377

Identifying Malicious Traffic on the Network  377

Signature-Based IPS/IDS  377

Policy-Based IPS/IDS  378

Anomaly-Based IPS/IDS  378

Reputation-Based IPS/IDS  378

When Sensors Detect Malicious Traffic  379

Controlling Which Actions the Sensors Should Take  381

Implementing Actions Based on the Risk Rating  382

IPv6 and IPS  382

Circumventing an IPS/IDS  382

Managing Signatures  384

Signature or Severity Levels  384

Monitoring and Managing Alarms and Alerts  385

Security Intelligence  385

IPS/IDS Best Practices  386

Exam Preparation Tasks  387

Review All the Key Topics  387
Complete the Tables and Lists from Memory 387
Define Key Terms 387

**Chapter 16 Implementing IOS-Based IPS 389**

“Do I Know This Already?” Quiz 389
Foundation Topics 392
Understanding and Installing an IOS-Based IPS 392
  - What Can IOS IPS Do? 392
  - Installing the IOS IPS Feature 393
  - Getting to the IPS Wizard 394
Working with Signatures in an IOS-Based IPS 400
  - Actions That May Be Taken 405
  - Best Practices When Tuning IPS 412
Managing and Monitoring IPS Alarms 412
Exam Preparation Tasks 417
Review All the Key Topics 417
Complete the Tables and Lists from Memory 417
Define Key Terms 417
Command Reference to Check Your Memory 418

**Part IV Using VPNs for Secure Connectivity 421**

**Chapter 17 Fundamentals of VPN Technology 423**

“Do I Know This Already?” Quiz 423
Foundation Topics 426
Understanding VPNs and Why We Use Them 426
  - What Is a VPN? 426
  - Types of VPNs 427
  - Two Main Types of VPNs 427
Main Benefits of VPNs 427
  - Confidentiality 428
  - Data Integrity 428
  - Authentication 430
  - Antireplay 430
Cryptography Basic Components 430
  - Ciphers and Keys 430
  - Ciphers 430
  - Keys 431
  - Block and Stream Ciphers 431
  - Block Ciphers 432
**Stream Ciphers** 432
Symmetric and Asymmetric Algorithms 432
*Symmetric* 432
*Asymmetric* 433
Hashes 434
Hashed Message Authentication Code 434
Digital Signatures 435
*Digital Signatures in Action* 435
Key Management 436
IPsec and SSL 436
*IPsec* 436
*SSL* 437

Exam Preparation Tasks 439
Review All the Key Topics 439
Complete the Tables and Lists from Memory 439
Define Key Terms 439

**Chapter 18 Fundamentals of the Public Key Infrastructure** 441

“Do I Know This Already?” Quiz 441

Foundation Topics 444
Public Key Infrastructure 444
Public and Private Key Pairs 444
RSA Algorithm, the Keys, and Digital Certificates 445
*Who Has Keys and a Digital Certificate?* 445
*How Two Parties Exchange Public Keys* 445
*Creating a Digital Signature* 445
Certificate Authorities 446
Root and Identity Certificates 446
*Root Certificate* 446
*Identity Certificate* 448
*Using the Digital Certificates to get the Peer’s Public Key* 448
*X.500 and X.509v3 Certificates* 449
Authenticating and Enrolling with the CA 450
Public Key Cryptography Standards 450
Simple Certificate Enrollment Protocol 451
Revoked Certificates 451
Uses for Digital Certificates 452
PKI Topologies 452
*Single Root CA* 453
Hierarchical CA with Subordinate CAs 453
Cross-Certifying CAs 453
Putting the Pieces of PKI to Work 453
  Default of the ASA 454
  Viewing the Certificates in ASDM 455
  Adding a New Root Certificate 455
  Easier Method for Installing Both Root and Identity certificates 457
Exam Preparation Tasks 462
Review All the Key Topics 462
Complete the Tables and Lists from Memory 462
Define Key Terms 463
Command Reference to Check Your Memory 463

Chapter 19 Fundamentals of IP Security 465
“Do I Know This Already?” Quiz 465
Foundation Topics 468
  IPsec Concepts, Components, and Operations 468
    The Goal of IPsec 468
    The Play by Play for IPsec 469
    Step 1: Negotiate the IKE Phase 1 Tunnel 469
    Step 2: Run the DH Key Exchange 471
    Step 3:Authenticate the Peer 471
    What About the User's Original Packet? 471
    Leveraging What They Have Already Built 471
    Now IPsec Can Protect the User's Packets 472
    Traffic Before IPsec 472
    Traffic After IPsec 473
    Summary of the IPsec Story 474
Configuring and Verifying IPsec 475
  Tools to Configure the Tunnels 475
  Start with a Plan 475
  Applying the Configuration 475
  Viewing the CLI Equivalent at the Router 482
  Completing and Verifying IPsec 484
Exam Preparation Tasks 491
Review All the Key Topics 491
Complete the Tables and Lists from Memory 491
Define Key Terms 492
Command Reference to Check Your Memory 492
Chapter 20  Implementing IPsec Site-to-Site VPNs  495
“Do I Know This Already?” Quiz  495
Foundation Topics  498
Planning and Preparing an IPsec Site-to-Site VPN  498
  Customer Needs  498
  Planning IKE Phase 1  500
  Planning IKE Phase 2  501
Implementing and Verifying an IPsec Site-to-Site VPN  502
  Troubleshooting IPsec Site-to-Site VPNs  511
Exam Preparation Tasks  526
Review All the Key Topics  526
Complete the Tables and Lists from Memory  526
Define Key Terms  526
Command Reference to Check Your Memory  526

Chapter 21  Implementing SSL VPNs Using Cisco ASA  529
“Do I Know This Already?” Quiz  529
Foundation Topics  532
Functions and Use of SSL for VPNs  532
  Is IPsec Out of the Picture?  532
  SSL and TLS Protocol Framework  533
  The Play by Play of SSL for VPNs  534
SSL VPN Flavors  534
Configuring SSL Clientless VPNs on ASA  535
  Using the SSL VPN Wizard  536
  Digital Certificates  537
  Authenticating Users  538
  Logging In  541
  Seeing the VPN Activity from the Server  543
Configuring the Full SSL AnyConnect VPN on the ASA  544
  Types of SSL VPNs  545
  Configuring Server to Support the AnyConnect Client  545
  Groups, Connection Profiles, and Defaults  552
  One Item with Three Different Names  553
  Split Tunneling  554
Exam Preparation Tasks  556
Review All the Key Topics  556
Complete the Tables and Lists from Memory  556
Define Key Terms  556
**Chapter 22**  **Final Preparation**  559  
- Tools for Final Preparation  559  
  - Pearson IT Certification Practice Test Engine and Questions on the CD  559  
  - Installing the Software from the CD  560  
  - Activating and Downloading the Practice Exam  560  
  - Activating Other Exams  560  
  - Premium Edition  561  
  - The Cisco Learning Network  561  
  - Memory Tables  561  
  - Chapter-Ending Review Tools  561  
  - Videos  562  
- Suggested Plan for Final Review/Study  562  
  - Using the Exam Engine  562  
- Summary  563  

**Part V**  **Appendixes**  565  
- A  **Answers to the “Do I Know This Already?” Quizzes**  567  
- B  **CCNA Security 640-554 (IINSv2) Exam Updates**  573  
  - Glossary  577  
- Index  587  

**On the CD**  
- C  **Memory Tables**  3  
- D  **Memory Tables Answer Key**  33
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.
Introduction

Congratulations! If you are reading this, you have in your possession a powerful tool that can help you to

- Improve your awareness and knowledge of network security
- Increase your skill level related to the implementation of that security
- Prepare for the CCNA Security certification exam

When writing this book, it was done with you in mind, and together we will discover the critical ingredients that make up the recipe for a secure network and work through examples of how to implement these features. By focusing on both covering the objectives for the CCNA Security exam and integrating that with real-world best practices and examples, Scott Morris and I created this content with the intention of being your personal tour guides, as we take you on a journey through the world of network security.

The 640-554 Implementing Cisco IOS Network Security (IINSv2) exam is required for the CCNA Security certification. The prerequisite for CCNA Security is the CCNA Route/Switch certification (or any CCIE certification). The CCNA Security exam tests your knowledge of securing Cisco routers and switches and their associated networks, and this book prepares you for that exam. This book covers all the topics listed in Cisco's exam blueprint, and each chapter includes key topics and preparation tasks to assist you in mastering this information. The CD that accompanies this book also includes bonus videos to assist you in your journey toward becoming a CCNA in Security. Of course, the CD included with the printed book also includes several practice questions to help you prepare for the exam.

About the 640-554 Implementing Cisco IOS Network Security (IINSv2) Exam

Cisco's objective of the CCNA Security exam is to verify the candidate’s understanding, implementation, and verification of security best practices on Cisco hardware and software. The focus points for the exam (which this book prepares you for) are as follows:

- Cisco routers and switches
  - Common threats, including blended threats, and how to mitigate them.
  - The lifecycle approach for a security policy
  - Understanding and implementing network foundation protection for the control, data, and management planes
  - Understanding, implementing, and verifying AAA (authentication, authorization, and accounting), including the details of TACACS+ and RADIUS
  - Understanding and implementing basic rules inside of Cisco Access Control Server (ACS) Version 5.x, including configuration of both ACS and a router for communications with each other
Standard, extended, and named access control lists used for packet filtering and for the classification of traffic

Understanding and implementing protection against Layer 2 attacks, including CAM table overflow attacks, and VLAN hopping

Cisco firewall technologies

Understanding and describing the various methods for filtering implemented by firewalls, including stateful filtering. Compare and contrast the strengths and weaknesses of the various firewall technologies.

Understanding the methods that a firewall may use to implement Network Address Translation (NAT) and Port Address Translation (PAT).

Understanding, implementing, and interpreting a Zone-Based Firewall policy through Cisco Configuration Professional (CCP).

Understanding and describing the characteristics and defaults for interfaces, security levels, and traffic flows on the Adaptive Security Appliance (ASA).

Implementing and interpreting a firewall policy on an ASA through the GUI tool named the ASA Security Device Manager (ASDM).

Intrusion prevention systems

Comparing and contrasting intrusion prevention systems (IPS) versus intrusion detection systems (IDS), including the pros and cons of each and the methods used by these systems for identifying malicious traffic

Describing the concepts involved with IPS included true/false positives/negatives

Configuring and verifying IOS-based IPS using CCP

VPN technologies

Understanding and describing the building blocks used for virtual private networks (VPN) today, including the concepts of symmetrical, asymmetrical, encryption, hashing, Internet Key Exchange (IKE), public key infrastructure (PKI), authentication, Diffie-Hellman, certificate authorities, and so on

Implementing and verifying IPsec VPNs on IOS using CCP and the command-line interface (CLI)

Implementing and verifying Secure Sockets Layer (SSL) VPNs on the ASA firewall using ASDM

As you can see, it is an extensive list, but together we will not only address and learn each of these, but we will also have fun doing it.

You can take the exam at Pearson VUE testing centers. You can register with VUE at http://www.vue.com/cisco/.
### 640-554 IINSv2 Exam

Table I-1 lists the topics of the 640-554 IINSv2 exam and indicates the parts in the book where these topics are covered.

<table>
<thead>
<tr>
<th>Exam Topic</th>
<th>Part</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Common Security Threats</strong></td>
<td></td>
</tr>
<tr>
<td>Describe common security threats</td>
<td>I, II, III</td>
</tr>
<tr>
<td><strong>Security and Cisco Routers</strong></td>
<td></td>
</tr>
<tr>
<td>Implement security on Cisco routers</td>
<td>II, III</td>
</tr>
<tr>
<td>Describe securing the control, data, and management plane</td>
<td>II</td>
</tr>
<tr>
<td>Describe Cisco Security Manager</td>
<td>II, III</td>
</tr>
<tr>
<td>Describe IPv4 to IPv6 transition</td>
<td>II</td>
</tr>
<tr>
<td><strong>AAA on Cisco Devices</strong></td>
<td></td>
</tr>
<tr>
<td>Implement AAA (authentication, authorization, and accounting)</td>
<td>II</td>
</tr>
<tr>
<td>Describe TACACS+</td>
<td>II</td>
</tr>
<tr>
<td>Describe RADIUS</td>
<td>II</td>
</tr>
<tr>
<td>Describe AAA</td>
<td>II</td>
</tr>
<tr>
<td>Verify AAA functionality</td>
<td>II</td>
</tr>
<tr>
<td><strong>IOS ACLs</strong></td>
<td></td>
</tr>
<tr>
<td>Describe standard, extended, and named IP IOS access control lists (ACLs) to filter packets</td>
<td>III</td>
</tr>
<tr>
<td>Describe considerations when building ACLs</td>
<td>III</td>
</tr>
<tr>
<td>Implement IP ACLs to mitigate threats in a network</td>
<td>III</td>
</tr>
<tr>
<td><strong>Secure Network Management and Reporting</strong></td>
<td></td>
</tr>
<tr>
<td>Describe secure network management</td>
<td>II</td>
</tr>
<tr>
<td>Implement secure network management</td>
<td>II</td>
</tr>
<tr>
<td><strong>Common Layer 2 Attacks</strong></td>
<td></td>
</tr>
<tr>
<td>Describe Layer 2 security using Cisco switches</td>
<td>II</td>
</tr>
<tr>
<td>Describe VLAN security</td>
<td>II</td>
</tr>
<tr>
<td>Implement VLANs and trunking</td>
<td>II</td>
</tr>
<tr>
<td>Implement spanning tree (securely)</td>
<td>II</td>
</tr>
<tr>
<td><strong>Cisco Firewall Technologies</strong></td>
<td></td>
</tr>
<tr>
<td>Exam Topic</td>
<td>Part</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Describe operational strengths and weaknesses of the different firewall</td>
<td>III</td>
</tr>
<tr>
<td>technologies</td>
<td></td>
</tr>
<tr>
<td>Describe stateful firewalls</td>
<td>III</td>
</tr>
<tr>
<td>Describe the types of NAT used in firewall technologies</td>
<td>III</td>
</tr>
<tr>
<td>Implement zone-based policy firewall using CCP</td>
<td>III</td>
</tr>
<tr>
<td>Implement the Cisco Adaptive Security Appliance (ASA)</td>
<td>III</td>
</tr>
<tr>
<td>Implement Network Address Translation (NAT) and Port Address Translation</td>
<td>III</td>
</tr>
<tr>
<td>(PAT)</td>
<td></td>
</tr>
<tr>
<td><strong>Cisco IPS</strong></td>
<td></td>
</tr>
<tr>
<td>Describe Cisco Intrusion Prevention System (IPS) deployment considerations</td>
<td>III</td>
</tr>
<tr>
<td>Describe IPS technologies</td>
<td>III</td>
</tr>
<tr>
<td>Configure Cisco IOS IPS using CCP</td>
<td>III</td>
</tr>
<tr>
<td><strong>VPN Technologies</strong></td>
<td></td>
</tr>
<tr>
<td>Describe the different methods used in cryptography</td>
<td>IV</td>
</tr>
<tr>
<td>Describe VPN technologies</td>
<td>IV</td>
</tr>
<tr>
<td>Describe the building blocks of IPsec</td>
<td>IV</td>
</tr>
<tr>
<td>Implement an IOS IPsec site-to-site VPN with pre-shared key authentication</td>
<td>IV</td>
</tr>
<tr>
<td>Verify VPN operations</td>
<td>IV</td>
</tr>
<tr>
<td>Implement Secure Sockets Layer (SSL) VPN using ASA Device Manager</td>
<td>IV</td>
</tr>
</tbody>
</table>

**About the Implementing Cisco IOS Network Security (IINSv2) 640-554 Official Cert Guide**

This book maps to the topic areas of the 640-554 exam and uses a number of features to help you understand the topics and prepare for your exam.

**Objectives and Methods**

This book uses several key methodologies to help you discover the exam topics for which you need more review, to help you fully understand and remember those details, and to help you prove to yourself that you have retained your knowledge of those topics. So, this book does not try to help you pass the exams only by memorization, but by truly learning and understanding the topics. This book is designed to assist you in the exam by using the following methods:

- Using a conversational style that reflects the fact that we wrote this book as if we made it just for you, as a friend, discussing the topics with you, one step at a time.
■ Helping you discover which exam topics you may want to invest more time studying, to really “get it”
■ Providing explanations and information to fill in your knowledge gaps
■ Supplying three bonus videos (on the CD) to reinforce some of the critical concepts and techniques that you have learned from in your study of this book
■ Providing practice questions to assess your understanding of the topics

Book Features

To help you customize your study time using this book, the core chapters have several features that help you make the best use of your time:

■ “Do I Know This Already?” quiz: Each chapter begins with a quiz that helps you determine how much time you need to spend studying that chapter.
■ Foundation Topics: These are the core sections of each chapter. They explain the concepts for the topics in that chapter.
■ Exam Preparation Tasks: After the “Foundation Topics” section of each chapter, the “Exam Preparation Tasks” section lists a series of study activities that you should do when you finish the chapter. Each chapter includes the activities that make the most sense for studying the topics in that chapter:
  ■ Review All the Key Topics: The Key Topic icon appears next to the most important items in the “Foundation Topics” section of the chapter. The “Review All the Key Topics” activity lists the key topics from the chapter, along with their page numbers. Although the contents of the entire chapter could be on the exam, you should definitely know the information listed in each key topic, so you should review these.
  ■ Complete the Tables and Lists from Memory: To help you memorize some lists of facts, many of the more important lists and tables from the chapter are included in a document on the CD. This document lists only partial information, allowing you to complete the table or list.
  ■ Define Key Terms: Although the exam is unlikely to ask a “define this term” type of question, the CCNA exams do require that you learn and know a lot of networking terminology. This section lists the most important terms from the chapter, asking you to write a short definition and compare your answer to the glossary at the end of the book.
  ■ Command Reference to Check Your Memory: Review important commands covered in the chapter.
■ CD-based practice exam: The companion CD contains an exam engine that enables you to review practice exam questions. Use these to prepare with a sample exam and to pinpoint topics where you need more study.
How This Book Is Organized

This book contains 21 core chapters. Chapter 22 includes some preparation tips and suggestions for how to approach the exam. Each core chapter covers a subset of the topics on the CCNA Security exam. The core chapters are organized into parts. They cover the following topics:

Part I: Fundamentals of Network Security

- **Chapter 1, “Networking Security Concepts”**: This chapter covers the need for and the building blocks of network and information security, threats to our networks today, and fundamental principles of secure network design.
- **Chapter 2, “Understanding Security Policies Using a Lifecycle Approach”**: This chapter covers risk analysis and management and security policies.
- **Chapter 3, “Building a Security Strategy”**: This chapter covers securing borderless networks and controlling and containing data loss.

Part II: Protecting the Network Infrastructure

- **Chapter 4, “Network Foundation Protection”**: This chapter covers introduction to securing the network using the network foundation protection (NFP) approach, the management plane, the control plane, and the data plane.
- **Chapter 5, “Using Cisco Configuration Professional to Protect the Network Infrastructure”**: This chapter covers introduction to Cisco Configuration Professional, CCP features and the GUI, setting up a new devices, CCP building blocks, and CCP audit features.
- **Chapter 6, “Securing the Management Plane on Cisco IOS Devices”**: This chapter covers management traffic and how to make it more secure and the implementation of security measures to protect the management plane.
- **Chapter 7, “Implementing AAA Using IOS and the ACS Server”**: This chapter covers the role of Cisco Secure ACS and the two primary protocols used with it, RADIUS and TACACS. It also covers configuration of a router to interoperate with an ACS server and configuration of the ACS server to interoperate with a router. The chapter also covers router tools to verify and troubleshoot router-to-ACS server interactions.
- **Chapter 8, “Securing Layer 2 Technologies”**: This chapter covers VLANs and trunking fundamentals, spanning-tree fundamentals, and common Layer 2 threats and how to mitigate them.
- **Chapter 9, “Securing the Data Plane in IPv6”**: This chapter covers IPv6 (basics, configuring, and developing a security plan for IPv6).

Part III: Mitigating and Controlling Threats

- **Chapter 10, “Planning a Threat Control Strategy”**: This chapter covers the design considerations for threat mitigation and containment and the hardware, software, and services used to implement a secure network.
Chapter 11, “Using Access Control Lists for Threat Mitigation”: This chapter covers the benefits and fundamentals for access control lists (ACL), implementing IPv4 ACLs as packet filters, and implementing IPv6 ACLs as packet filters.

Chapter 12, “Understanding Firewall Fundamentals”: This chapter covers firewall concepts and the technologies used by them, including the function of Network Address Translation (NAT), including its building blocks, and the guidelines and considerations for creating and deploying firewalls.

Chapter 13, “Implementing Cisco IOS Zone-Based Firewalls”: This chapter covers the operational and functional components of the IOS Zone-Based Firewall and how to configure and verify the IOS Zone-Based Firewall.

Chapter 14, “Configuring Basic Firewall Policies on Cisco ASA”: This chapter covers the Adaptive Security Appliance (ASA) family and features, ASA firewall fundamentals, and configuring the ASA.

Chapter 15, “Cisco IPS/IDS Fundamentals”: This chapter compares intrusion prevention systems (IPS) to intrusion detection systems (IDS) and covers how to identify malicious traffic on the network, manage signatures, and monitor and manage alarms and alerts.

Chapter 16, “Implementing IOS-Based IPS”: This chapter covers the features included in IOS-based IPS (in software) and installing the IPS feature, working with signatures in IOS-based IPS, and managing and monitoring IPS alarms.

Part IV: Using VPNs for Secure Connectivity

Chapter 17, “Fundamentals of VPN Technology”: This chapter covers what VPNs are and why we use them and the basic ingredients of cryptography.

Chapter 18, “Fundamentals of the Public Key Infrastructure”: This chapter covers the concepts, components, and operations of the public key infrastructure (PKI) and includes an example of putting the pieces of PKI to work.

Chapter 19, “Fundamentals of IP Security”: This chapter covers the concepts, components, and operations of IPsec and how to configure and verify IPsec.

Chapter 20, “Implementing IPsec Site-to-Site VPNs”: This chapter covers planning and preparing to implement an IPsec site-to-site VPN and implementing and verifying the IPsec site-to-site VPN.

Chapter 21, “Implementing SSL VPNs Using Cisco ASA”: This chapter covers the functions and use of SSL for VPNs, configuring SSL clientless VPN on the ASA, and configuring the full SSL AnyConnect VPN on the ASA.

Chapter 22, “Final Preparation”: This chapter identifies tools for final exam preparation and helps you develop an effective study plan.

Appendixes

Appendix A, “Answers to the ‘Do I Know This Already?’ Quizzes”: Includes the answers to all the questions from Chapters 1 through 21.
Appendix B, “CCNA Security 640-554 (IINSv2) Exam Updates”: This appendix provides instructions for finding updates to the exam and this book when and if they occur.

CD-Only Appendixes

Appendix C, “Memory Tables”: This CD-only appendix contains the key tables and lists from each chapter, with some of the contents removed. You can print this appendix and, as a memory exercise, complete the tables and lists. The goal is to help you memorize facts that can be useful on the exams. This appendix is available in PDF format on the CD; it is not in the printed book.

Appendix D, “Memory Tables Answer Key”: This CD-only appendix contains the answer key for the memory tables in Appendix C. This appendix is available in PDF format on the CD; it is not in the printed book.

Premium Edition eBook and Practice Test

This Cert Guide contains a special offer for a 70% discount off the companion CCNA Security 640-554 Official Cert Guide Premium Edition eBook and Practice Test. The Premium Edition combines an eBook version of the text with an enhanced Pearson IT Certification Practice Test. By purchasing the Premium Edition, you get access to two eBook versions of the text: a PDF version and an EPUB version for reading on your tablet, eReader, or mobile device. You also get an enhanced practice test that contains an additional two full practice tests of unique questions. In addition, all the practice test questions are linked to the PDF eBook, allowing you to get more detailed feedback on each question instantly. To take advantage of this offer, you will need the coupon code included on the paper in the CD sleeve. Just follow the purchasing instructions that accompany the code to download and start using your Premium Edition today!
This page intentionally left blank
This chapter covers the following subjects:

- Securing management traffic
- Implementing security measures to protect the management plane
Accessing and configuring Cisco devices is a common occurrence for an administrator. Malicious router management traffic from an unauthorized source can pose a security threat. For example, an attacker could compromise router security by intercepting login credentials (such as the username and password). This chapter introduces the concept of the management plane (which is a collection of protocols and access methods we use to configure, manage, and maintain a network device) and examines how to protect it.

“Do I Know This Already?” Quiz

The “Do I Know This Already?” quiz helps you determine your level of knowledge of this chapter’s topics before you begin. Table 6-1 details the major topics discussed in this chapter and their corresponding quiz questions.

<table>
<thead>
<tr>
<th>Foundation Topics Section</th>
<th>Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Securing Management Traffic</td>
<td>1–4, 6</td>
</tr>
<tr>
<td>Implementing Security Measures to Protect the Management Plane</td>
<td>5, 7–10</td>
</tr>
</tbody>
</table>

1. Which one of the following follows best practices for a secure password?
   a. ABC123!
   b. SlE3peR1#
   c. tough-passfraze
   d. InterEstIng-PaSsWoRd
2. When you connect for the first time to the console port on a new router, which privilege level are you using initially when presented with the command-line interface?
   a. 0
   b. 1
   c. 15
   d. 16

3. Which of the following is not impacted by a default login authentication method list?
   a. AUX line
   b. HDLC interface
   c. Vty line
   d. Console line

4. You are trying to configure a method list, and your syntax is correct, but the command is not being accepted. Which of the following might cause this failure? (Choose all that apply.)
   a. Incorrect privilege level
   b. AAA not enabled
   c. Wrong mode
   d. Not allowed by the view

5. Cisco recommends which version of Simple Network Management Protocol (SNMP) on your network if you need it?
   a. Version 1
   b. Version 2
   c. Version 3
   d. Version 4

6. How can you implement role-based access control (RBAC)? (Choose all that apply.)
   a. Provide the password for a custom privilege level to users in a given role
   b. Associate user accounts with specific views
   c. Use access lists to specify which devices can connect remotely
   d. Use AAA to authorize specific users for specific sets of permissions
7. Which of the following indirectly requires the administrator to configure a host name?
   a. Telnet
   b. HTTP
   c. HTTPS
   d. SSH

8. What are the two primary benefits of using NTP along with a syslog server? (Choose all that apply.)
   a. Correlation of syslog messages from multiple different devices
   b. Grouping of syslog messages into summary messages
   c. Synchronization in the sending of syslog messages to avoid congestion
   d. Accurate accounting of when a syslog message occurred

9. Which of the following commands result in a secure bootset? (Choose all that apply.)
   a. secure boot-set
   b. secure boot-config
   c. secure boot-files
   d. secure boot-image

10. What is a difference between a default and named method list?
   a. A default method list can contain up to four methods.
   b. A named method list can contain up to four methods.
   c. A default method list must be assigned to an interface or line.
   d. A named method list must be assigned to an interface or line.
Foundation Topics

Securing Management Traffic

It is tricky to fix a problem if you are unaware of the problem. So, this first section starts by classifying and describing management traffic and identifying some of the vulnerabilities that exist. It also identifies some concepts that can help you to protect that traffic. This chapter then provides implementation examples of the concepts discussed earlier.

What Is Management Traffic and the Management Plane?

When you first get a new router or switch, you connect to it for management using a blue rollover cable that connects from your computer to the console port of that router or switch. This is your first exposure to the concept of management traffic. By default, when you connect to a console port you are not prompted for a username or any kind of password. By requiring a username or password, you are taking the first steps toward improving what is called the management plane on this router or switch.

The management plane includes not only configuration of a system, but also who may access a system and what they are allowed to do while they are logged in. The management plane also includes messages to or from a Cisco router or switch that is used to maintain or report on the current status of the device, such as a management protocol like Simple Network Management Protocol (SNMP).

Beyond the Blue Rollover Cable

Using the blue rollover cable directly connected to the console port is fairly safe. Unfortunately, it is not very convenient to require the use of a console port when you are trying to manage several devices that are located in different buildings, or on different floors of the same building. A common solution to this problem is to configure the device with an IP address that you can then use to connect to that device remotely. It is at this moment that the security risk goes up. Because you are connecting over IP, it might be possible for an unauthorized person to also connect remotely. The management plane, if it were secure, would enable you to control who may connect to manage the box, when they may connect, what they may do, and report on anything that they did. At the same time, you want to ensure that all the packets that go between the device being managed and the computer where the administrator is sitting are encrypted so that anyone who potentially may capture the individual packets while going through the network could not interpret the contents of the packets (which might contain sensitive information about the configuration or passwords used for access).
Management Plane Best Practices

When implementing a network, remember the following best practices. Each one, when implemented, improves the security posture of the management plane for your network:

- **Strong passwords:** Make passwords very difficult to break. Whenever you use passwords, make them complex and difficult to guess. An attacker can break a password in several ways, including a dictionary and/or a brute force attack. A dictionary attack automates the process of attempting to log in as the user, running through a long list of words (potential passwords); when one attempt fails, the attack just tries the next one (and so on). A brute-force attack doesn't use a list of words, but rather tries thousands or millions of possible character strings trying to find a password match (modifying its guesses progressively if it incorrectly guesses the password or stops before it reaches the boundary set by the attacker regarding how many characters to guess, with every possible character combination being tried.). A tough password takes longer to break than a simple password.

- **User authentication and AAA:** Require administrators to authenticate using usernames and passwords. This is much better than just requiring a password and not knowing exactly who the user is. To require authentication using usernames and passwords, you can use a method authentication, authorization, and accounting (AAA). Using this, you can control which administrators are allowed to connect to which devices and what they can do while they are there, and you can create an audit trail (accounting records) to document what they actually did while they were logged in.

- **Role-based access control (RBAC):** Not every administrator needs full access to every device, and you can control this through AAA and custom privilege levels/parser views. For example, if there are junior administrators, you might want to create a group that has limited permissions. You could assign users who are junior administrators to that group; they then inherit just those permissions. This is one example of using RBAC. Another example of RBAC is creating a custom privilege level and assigning user accounts to that level. Regardless of how much access an administrator has, a change management plan for approving, communicating, and tracking configuration changes should be in place and used before changes are made.

- **Encrypted management protocols:** When using either in-band or out-of-band management, encrypted communications should be used, such as Secure Shell (SSH) or Hypertext Transfer Protocol Secure (HTTPS). Out-of-band (OOB) management implies that there is a completely separate network just for management protocols and a different network for end users and their traffic. In-band management is when the packets used by your management protocols may intermingle with the user packets (considered less secure than OOB). Whether in-band or OOB, if a plaintext management protocol must be used, such as Telnet or HTTP, use it in combination with a virtual private network (VPN) tunnel that can encrypt and protect the contents of the packets being used for management.
- **Logging**: Logging is a way to create an audit trail. Logging includes not only what administrators have changed or done, but also system events that are generated by the router or switch because of some problem that has occurred or some threshold that has been reached. Determine the most important information to log, and identify logging levels to use. A logging level simply specifies how much detail to include in logging messages, and may also indicate that some less-serious logging messages do not need to be logged. Because the log messages may include sensitive information, the storage of the logs and the transmission of the logs should be protected to prevent tampering or damage. Allocate sufficient storage capacity for anticipated logging demands. Logging may be done in many different ways, and your logging information may originate from many different sources, including messages that are automatically generated by the router or switch and sent to a syslog server. A syslog server is a computer that is set up to receive and store syslog messages generated from network devices. If SNMP is used, preferably use Version 3 because of its authentication and encryption capabilities. You can use SNMP to change information on a router or switch, and you can also use it to retrieve information from the router or switch. An **SNMP trap** is a message generated by the router or switch to alert the manager or management station of some event.

- **Network Time Protocol (NTP)**: Use NTP to synchronize the clocks on network devices so that any logging that includes time stamps may be easily correlated. Preferably, use NTP Version 3, to leverage its ability to provide authentication for time updates. This becomes very important to correlate logs between devices in case there is ever a breach and you need to reconstruct (or prove in a court of law) what occurred.

- **Secure system files**: Make it difficult to delete, whether accidentally or on purpose, the startup configuration files and the IOS images that are on the file systems of the local routers and switches. You can do so by using built-in IOS features discussed later in this chapter.

---

**Note**  Even though OOB management is usually preferred over in-band management, some management applications benefit from in-band management. For example, consider a network management application that checks the reachability of various hosts and subnets. To check this reachability, an application might send a series of pings to a remote IP address, or check the availability of various Layer 4 services on a remote host. To perform these “availability” checks, the network management application needs to send traffic across a production data network. Also, in-band network management often offers a more economic solution for smaller networks. Even if using in-band management, it should be a separate subnet/VLAN, and one that only a select few people/devices have access to get to. This reduces your footprint for possible attack vectors.
Chapter 6: Securing the Management Plane on Cisco IOS Devices

Password Recommendations

Using passwords is one way to provide access. Using passwords alone is not as good as requiring a user ID or login name associated with the password for a user.

Here are some guidelines for password creation:

- It is best to have a minimum of eight characters for a password; bigger is better. This rule can be enforced by the local router if you are storing usernames and passwords on the router in the running config. The command `security passwords min-length` followed by the minimum password length enforces this rule on new passwords that are created, including the enable secret and line passwords on the vty, AUX, and console 0. Preexisting passwords will still operate even if they are less than the new minimum specified by the command.

- Passwords can include any alphanumeric character, a mix of uppercase and lowercase characters, and symbols and spaces. As a general security rule, passwords should not use words that may be found in a dictionary, because they are easier to break. Leading spaces in a password are ignored, but any subsequent spaces, including in the middle or at the end of a password, literally become part of that password and are generally a good idea. Another good practice is using special characters or even two different words (that are not usually associated with each other) as a passphrase when combined together. Caution should be used to not require such a complex password that the user must write it down to remember it, which increases the chance of it becoming compromised.

- Passwords in a perfect environment should be fairly complex, and should be changed periodically. The frequency of requiring a change in passwords depends on your security policy. Passwords changed often are less likely to be compromised.

- From a mathematical perspective, consider how many possibilities someone would need to try to guess a password. If only capital letters are used, you have 26 possibilities for each character. If your password is one character long, that is 26, or 26 possible variants. If you have a two-character password, that is 262, or 676 possible variants. If you start using uppercase (26) and lowercase (26), numerals (10), and basic special characters (32), your starting set becomes 94 possible variants per character. Even if we look at using an eight-character password, that is 948 or 6,095,689,385,410,816 (6.1 quadrillion) possibilities.

Using AAA to Verify Users

Unauthorized user access to a network creates the potential for network intruders to gain information or cause harm or both. Authorized users need access to their network resources, and network administrators need access to the network devices to configure and manage them. AAA offers a solution for both. In a nutshell, the goal of AAA is to identify who users are before giving them any kind of access to the network, and once they are identified, only give them access to the part they are authorized to use, see, or manage. AAA can create an audit trail that identifies exactly who did what and when
they did it. That is the spirit of AAA. User accounts may be kept on the local database or on a remote server. The local database is a fancy way of referring to user accounts that are created on the local router and are part of the running configuration.

### AAA Components

Providing network and administrative access in a Cisco environment—regardless of whether it involves administrators managing the network or users getting access through network resources—is based on a modular architecture composed of the following three functional components:

- **Authentication**: Authentication is the process by which individuals prove that they are who they claim to be. The network environment has a variety of mechanisms for providing authentication, including the use of a username and password, token cards, and challenge and response. A common use is authenticating an administrator's access to a router console port, auxiliary port, or vty lines. An analogy is a bank asking you to prove that you are who you say you are before allowing you to make a transaction. As an administrator, you can control how a user is authenticated. Choices include referring to the local running configuration on the router to look for the username, going to an external server that holds the username and password information, and other methods. To specify the method to use, you create an authentication “method list” that specifies how to authenticate the user. There can be custom named method lists or default method lists. Examples of each are shown later in this chapter.

- **Authorization**: After the user or administrator has been authenticated, authorization can be used to determine which resources the user or administrator is allowed to access, and which operations may be performed. In the case of the average user, this might determine what hours that user is allowed on the network. In the case of an administrator, it could control what the administrator is allowed to look at or modify. An analogy is a bank (after having already authenticated who you are) determining whether you are authorized to withdraw some amount of money (probably based on your balance in your account at the bank). You can create authorization method lists to specify how to authorize users on the network.

- **Accounting and auditing**: After being authenticated and possibly authorized, the user or administrator begins to access the network. It is the role of accounting and auditing to record what the user or administrator actually does with this access, what he accesses, and how long he accesses it. This is also known as creating an audit trail. An analogy is a bank documenting and debiting your account for the money you withdraw. You can create and assign accounting method lists to control what is accounted for and where the accounting records will be sent.

### Options for Storing Usernames, Passwords, and Access Rules

Cisco provides many ways to implement AAA services for Cisco devices, many of which use a centralized service to keep usernames, passwords, and configured rules about who can access which resources. Over the years, there have been many names and access methods
associated with the central server, including calling it an authentication server, AAA server, ACS server, TACACS server, or RADIUS server. These all refer to the same type of function: a server that contains usernames, passwords, and rules about what may be accessed. A router or switch acts like a client to this server and can send requests to the server to verify the credentials of an administrator or user who is trying to access a local router or switch. The following list describes a few of these centralized server types:

- **Cisco Secure ACS Solution Engine:** This is a dedicated server that contains the usernames, their passwords, and other information about what users are allowed to access and when. In the past, this was sold as a server appliance with the Access Control Server (ACS) software preinstalled. A router or switch becomes a client to the server. The router can be configured to require authentication from a user or administrator before providing access, and the router sends this request to the ACS server and lets the ACS server make the decision about allowing the user or administrator to continue. The protocol used between the router and the ACS server is normally TACACS+ if you are authenticating an administrator who is seeking command-line access. The protocol used between the router and the ACS server is normally RADIUS if you are authenticating an end user for network access. These are not hard-and-fast rules, and you can use either of the two protocols for similar features in many cases.

- **Cisco Secure ACS for Windows Server:** This software package may be used for user and administrator authentication. AAA services on the router or network access server (NAS) contact an external Cisco Secure ACS (running on a Microsoft Windows system). This is an older flavor of ACS, but may still be relevant to the certification exams.

- **Current flavors of ACS functionality:** The most common way that ACS services are implemented today is through a virtual machine running on some flavor of VMware. Another up-and-coming service to support similar services to ACS is called the Cisco Identity Services Engine (ISE), which can be bundled in a single physical or logical device or appliance.

- **Self-contained AAA:** AAA services may be self-contained in the router itself. Implemented in this fashion, this form of authentication and authorization is also known as local authentication and authorization. The database that contains the usernames and passwords is the running configuration of the router or IOS device, and from a AAA perspective is referred to as the local database on the router. So, if you create a user locally on the router, you can also say that you created a user in the local database of the router. It is the same thing. In this case, because the router is acting as its own AAA server, you do not use TACACS+ or RADIUS as a protocol to connect to a remote ACS server, because you are not using an ACS server.

### Authorizing VPN Users

One common implementation of AAA is its use in authenticating users accessing the corporate LAN through a remote-access IPsec VPN.
Let’s see how authentication and authorization applies to users who are trying to access our network through a VPN. The first step is to authenticate users to find out who they are, and after we find out who they are, we can then control what they are authorized for. For example, if a user connects via a VPN, that user may or may not be allowed access to certain portions of the network based on who the user is. This type of access is sometimes called packet mode, as in a user attempting to send packets through the network instead of trying to get a command-line interface (CLI) like an administrator would. A user connecting over a dial-up connection (older technology) could very likely be authenticated via a PPP connection using the same concepts. In either case, we authenticate the users by asking for their username and password, and then check the rules to see what they are authorized to access. If we use the remote Access Control Server (ACS) server for the authentication and authorization for an end user, we would very likely use the RADIUS protocol between the router and the AAA server.

AAA access control is supported using either a local username-password database or through a remote server (such as an ACS server). To provide access to a small group of network users, or as a backup in case the ACS server cannot be reached, a local security database can be configured in the router using the `username` command.

**Router Access Authentication**

Note that we must choose authentication first if we want to also use authorization for a user or administrator. We cannot choose authorization for a user without knowing who that user is through authentication first.

Typically, if we authenticate an administrator, we also authorize that administrator for what we want to allow him to do. Administrators traditionally are going to need access to the CLI. When an administrator is at the CLI, that interface is provided by something called an EXEC shell. If we want to authorize the router to provide this CLI, that is a perfect example of using AAA to first authenticate the user (in this case, the administrator) and then authorize that user to get a CLI prompt (the EXEC shell) and even place the administrator at the correct privilege level. This type of access (CLI) could also be referred to as character mode. Simply think of an administrator at a CLI typing in characters to assist you in remembering that this is “character” mode. With the administrator, we would very likely authenticate his login request and authorize that administrator to use an EXEC shell. If we were using a remote ACS server for this authentication and authorization of an administrator, we would very likely use TACACS+ (between the router and the ACS server) because it has the most granular control, compared with RADIUS, which is the alternative. TACACS+ and RADIUS are both discussed in another chapter of this book in greater detail.

Table 6-2 identifies some of the terms that refer to the type of access and the likely protocols used between the router acting as a client and the ACS server acting as the AAA server.
Table 6-2  AAA Components to Secure Administrative and Remote LAN Access

<table>
<thead>
<tr>
<th>Access Type</th>
<th>Mode</th>
<th>Where These Are Likely to Be Used</th>
<th>AAA Command Element</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote administrative access</td>
<td>Character (line or EXEC mode)</td>
<td>Lines: vty, AUX console, and tty</td>
<td>login, enable, exec</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote network access end users</td>
<td>Packet (interface mode) such as an interface with PPP requiring authentication</td>
<td>Interfaces: async, group-async, BRI, PRI, Other functionality: VPN user authentication</td>
<td>ppp, network, vpn groups</td>
</tr>
</tbody>
</table>

The AAA Method List

To make implementing AAA modular, we can specify individual lists of ways we want to authenticate, authorize, and account for the users. To do this, we create a method list that defines what resource will be used (such as the local database, an ACS server via TACACS+ protocol or an ACS server via RADIUS protocol, and so forth). To save time, we can create a default list or custom lists. We can create method lists that define the authentication methods to use, authorization method lists that define which authorization methods to use, and accounting method lists that specify which accounting method lists to use. A default list, if created, applies to the entire router or switch. A custom list, to be applied, must be both created and then specifically referenced in line or interface configuration mode. You can apply a custom list over and over again in multiple lines or interfaces. The type of the method list may be authentication, authorization, or accounting.

The syntax for a method list is as follows:

```
aaa type {default | list-name} method-1 [method-2 method-3 method-4]
```

The commands for a method list, along with their descriptions, are shown in Table 6-3.

Table 6-3  Method List Options

<table>
<thead>
<tr>
<th>Command Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>type</td>
<td>Identifies the type of list being created. Relevant options are authentication, authorization, or accounting.</td>
</tr>
<tr>
<td>default</td>
<td>Specifies the default list of methods to be used based on the methods that follow this argument. If you use the keyword default, a custom name is not used.</td>
</tr>
</tbody>
</table>
### Command Element   Description

<table>
<thead>
<tr>
<th>Command Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>list-name</td>
<td>Used to create a custom method list. This is the name of this list, and is used when this list is applied to a line, such as to vty lines 0–4.</td>
</tr>
<tr>
<td>method</td>
<td>At least one method must be specified. To use the local user database, use the local keyword. A single list can contain up to 4 methods, which are tried in order, from left to right. In the case of an authentication method list, methods include the following: enable: The enable password is used for authentication. This might be an excellent choice as the last method in a method list. This way, if the previous methods are not available (such as the AAA server, which might be down or not configured), the router times out on the first methods and eventually prompts the user for the enable secret as a last resort. krb5: Kerberos 5 is used for authentication. krb5-telnet: Kerberos 5 Telnet authentication protocol is used when using Telnet to connect to the router. line: The line password (the one configured with the password command, on the individual line) is used for authentication. local: The local username database (running config) is used for authentication. local-case: Requires case-sensitive local username authentication. none: No authentication is used. group radius: A RADIUS server (or servers) is used for authentication. group tacacs+: A TACACS+ server (or servers) is used for authentication. group group-name: Uses either a subset of RADIUS or TACACS+ servers for authentication as defined by the aaa group server radius or aaa group server tacacs+ command.</td>
</tr>
</tbody>
</table>

### Role-Based Access Control

The concept of role-based access control (RBAC) is to create a set of permissions or limited access and assign that set of permissions to users or groups. Those permissions are used by individuals for their given roles, such as a role of administrator or a role of a help desk person and so on. There are different ways to implement RBAC, including creating custom privilege levels and creating parser views (coming up later in this section). In either case, the custom level or view can be assigned the permissions needed for a specific
function or role, and then users can use those custom privilege levels or parser views to carry out their job responsibilities on the network, without being given full access to all configuration options.

**Custom Privilege Levels**

When you first connect to a console port on the router, you are placed into user mode. User mode is really privilege level 1. This is represented by a prompt that ends with `>`. When you move into privileged mode by typing the `enable` command, you are really moving into privilege level 15. A user at privilege level 15 has access and can issue all the commands that are attached to or associated with level 15 and below. Nearly all the configuration commands, and the commands that get us into configuration mode, are associated by default with privilege level 15.

By creating custom privilege levels (somewhere between levels 2 and 14, inclusive), and assigning commands that are normally associated with privilege level 15 to this new level, you can give this subset of new commands to the individual who either logs in at this custom level or to the user who logs in with a user account that has been assigned to that level.

**Limiting the Administrator by Assigning a View**

Working with individual commands and assigning them to custom privilege levels is tedious at best, and it is for that reason that method is not used very often. So, what can be done if we need users to have a subset of commands available to them, but not all of them? In an earlier chapter, we looked at how Cisco Configuration Professional (CCP) could restrict the visibility of the features in the navigation pane by using user profiles. This technique, however, did not protect the router against a user connecting with Telnet or SSH, and if that user had level 15 permissions, the router would once again be unprotected at the CLI.

A solution to this is to use parser views, also referred to as simply a view. You can create a view and associate it with a subset of commands. When the user logs in using this view, that same user is restricted to only being able to use the commands that are part of his current view. You can also associate multiple users with a single view.

**Encrypted Management Protocols**

It is not always practical to have console access to the Cisco devices you manage. There are several options for remote access via IP connectivity, and the most common is an application called Telnet. The problem with Telnet is that it uses plain text, and anyone who gets a copy of those packets can identify our usernames and passwords used for access and any other information that goes between administrator and the router being managed (over the management plane). One solution to this is to not use Telnet. If Telnet must be used, it should only be used out of band, or placed within a VPN tunnel for privacy, or both.
Secure Shell provides the same functionality as Telnet, in that it gives you a CLI to a router or switch; unlike Telnet, however, SSH encrypts all the packets used in the session. So, with SSH, if a packet is captured and viewed by an unauthorized individual, it will not have any meaning because the contents of each packet are encrypted and the attacker or unauthorized person will not have the keys or means to decrypt the information. The encryption provides the feature of confidentiality.

With security, bigger really is better. With SSH, Version 2 is bigger and better than Version 1. Either version, however, is better than the unencrypted Telnet protocol. When you type in `ip ssh version 2`, (to enable version 2), the device may respond with a Version “1.99” is active. This is a function of a server that runs 2.0 but also supports backward compatibility with older versions. For more information, see RFC4253, section 5.1. You should use SSH rather than Telnet whenever possible.

For GUI management tools such as CCP, use HTTPS rather than HTTP because it encrypts the session which provides confidentiality for the packets in that session.

**Using Logging Files**

I still recall an incident on a customer site when a database server had a failed disk and was running on its backup. It was like that for weeks until they noticed a log message. If a second failure had occurred, the results would have been catastrophic. Administrators should, on a regular basis, analyze logs, especially from their routers, in addition to logs from other network devices. Logging information can provide insight into the nature of an attack. Log information can be used for troubleshooting purposes. Viewing logs from multiple devices can provide event correlation information (that is, the relationship between events occurring on different systems). For proper correlation of events, accurate time stamps on those events are important. Accurate time can be implemented through Network Time Protocol (NTP).

Cisco IOS devices can send log output to a variety of destinations, including the following:

- **Console:** A router’s console port can send log messages to an attached terminal (such as your connected computer, running a terminal emulation program).

- **vty lines:** Virtual tty (vty) connections (used by SSH and Telnet connections) can also receive log information at a remote terminal (such as an SSH or Telnet client). However, the `terminal monitor` command should be issued to cause log messages to be seen by the user on that vty line.

- **Buffer:** When log messages are sent to a console or a vty line, those messages are not later available for detailed analysis. However, log messages can be stored in router memory. This “buffer” area can store messages up to the configured memory size, and then the messages are rotated out, with the first in being the first to be removed. When the router is rebooted, these messages in the buffer memory are lost.

- **SNMP server:** When configured as an SNMP device, a router or switch can generate log messages, in the form of SNMP traps and send them to an SNMP manager (server).
**Syslog server**: A popular choice for storing log information is a syslog server, which is easily configured and can store a large volume of logs. Syslog messages can be directed to one or more syslog servers from the router or switch.

A syslog logging solution consists of two primary components: syslog servers and syslog clients. A syslog server receives and stores log messages sent from syslog clients such as routers and switches.

Not all syslog messages are created equal. Specifically, they have different levels of severity. Table 6-4 lists the eight levels of syslog messages. The higher the syslog level, the more detailed the logs. Keep in mind that more-detailed logs require a bit more storage space, and also consider that syslog messages are transmitted in clear text. Also consider that the higher levels of syslog logging consume higher amounts of CPU processing time. For this reason, take care when logging to the console at the debugging level.

<table>
<thead>
<tr>
<th>Level</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Emergencies</td>
<td>System is unusable.</td>
</tr>
<tr>
<td>1</td>
<td>Alerts</td>
<td>Immediate action needed.</td>
</tr>
<tr>
<td>2</td>
<td>Critical</td>
<td>Critical conditions.</td>
</tr>
<tr>
<td>3</td>
<td>Errors</td>
<td>Error conditions.</td>
</tr>
<tr>
<td>4</td>
<td>Warnings</td>
<td>Warning conditions.</td>
</tr>
<tr>
<td>5</td>
<td>Notifications</td>
<td>Normal, but significant conditions.</td>
</tr>
<tr>
<td>6</td>
<td>Informational</td>
<td>Informational messages.</td>
</tr>
<tr>
<td>7</td>
<td>Debugging</td>
<td>Highly detailed information based on current debugging that is turned on.</td>
</tr>
</tbody>
</table>

The syslog log entries contain time stamps, which are helpful in understanding how one log message relates to another. The log entries include severity level information in addition to the text of the syslog messages. Having synchronized time on the routers, and including time stamps in the syslog messages, makes correlation of the syslog messages from multiple devices more meaningful.

**Understanding NTP**

*Network Time Protocol (NTP)* uses UDP port 123, and it allows network devices to synchronize their time. Ideally, they would synchronize their time to a trusted time server. You can configure a Cisco router to act as a trusted NTP server for the local network, and in the same way, that trusted NTP server could turn around and be an NTP client to a trusted NTP server either on the Internet or reachable via network connectivity. NTP Version 3 supports cryptographic authentication between NTP devices, and for this reason its use is preferable over any earlier versions.
One benefit of having reliable synchronized time is that log files and messages generated by the router can be correlated. In fact, if we had 20 routers, and they were all reporting various messages and all had the same synchronized time, we could very easily correlate the events across all 20 routers if we looked at those messages on a common server. A common server that is often used is a syslog server.

**Protecting Cisco IOS Files**

Similar to the computers that we use every day, a router also uses an operating system. The Cisco operating system on the router is called **IOS**. When a router first boots, it performs a power-on self-test, and then looks for an image of IOS on the flash. After loading the IOS into RAM, the router then looks for its startup configuration. If for whatever reason an IOS image or the startup configuration cannot be found or loaded properly, the router will effectively be nonfunctional as far as the network is concerned.

To help protect a router from accidental or malicious tampering of the IOS or startup configuration, Cisco offers a resilient configuration feature. This feature maintains a secure working copy of the router IOS image and the startup configuration files at all times. Once enabled, the administrator cannot disable the features remotely (but can if connected directly on the console). The secure files are referred to as a **secure bootset**.

**Implement Security Measures to Protect the Management Plane**

The first section of this chapter covered some best practices to protect the management plane. With that in mind, you can now leverage what you have learned and look at some practical examples of implementing those best practices. It requires both the understanding and implementation of these best practices to secure your networks.

**Implementing Strong Passwords**

The privileged EXEC secret (the one used to move from user mode to privileged mode) should not match any other password that is used on the system. Many of the other passwords are stored in plain text (such as passwords on the vty lines). If an attacker discovers these other passwords, he might try to use them to get into privileged mode, and that is why the enable secret should be unique. Service password encryption scrambles any plaintext passwords as they are stored in the configuration. This is useful for preventing someone who is looking over your shoulder from reading a plaintext password that is displayed in the configuration on the screen. Any new plaintext passwords are also scrambled as they are stored in the router’s configuration.

Example 6-1 shows the use of strong passwords.
Example 6-1  Using Strong Passwords

! Use the "secret" keyword instead of the "password" for users  
! This will create a secured password in the configuration by default 
! The secret is hashed using the MD5 algorithm as it is stored in the 
! configuration
R1(config)# username admin secret CeyeSc01$24

! At a minimum, require a login and password for access to the console port
! Passwords on lines, including the console, are stored as plain text, by
! default, in the configuration
R1(config)# line console 0
R1(config-line)# password k4(1fmMsS1#
R1(config-line)# login
R1(config-line)# exit

! At a minimum, require a login and password for access to the VTY lines which
! is where remote users connect when using Telnet
! Passwords on lines, including the vty lines, are stored as plain text, by
! default, in the configuration
R1(config)# line vty 0 4
R1(config-line)# password 8wT1*eGP5@
R1(config-line)# login

! At a minimum, require a login and password for access to the AUX line
! and disable the EXEC shell if it will not be used
R1(config-line)# line aux 0
R1(config-line)# no exec
R1(config-line)# password 1wT1@ecP27
R1(config-line)# login
R1(config-line)# exit

! Before doing anything else, look at the information entered.
R1(config)# do show run | include username
username admin secret 5 $1$XJdX$9hqvG53z31esPSBL0qggO.

R1(config)#
R1(config)# do show run | include password
no service password-encryption
password k4(1fmMsS1#
password 8wT1*eGP5@
password 1wT1@ecP27

R1(config)#
Notice that we can not determine the admin user's password, since it is automatically hashed using the MD5 algorithm because of using the secret command, however, we can still see all the other plain text passwords.

Encrypt the plain text passwords so that someone reading the configuration won't know what the passwords are by simply looking at the configuration.

R1(config)# service password-encryption

Verify that the plain text passwords configured are now scrambled due to the command "service password-encryption"

R1(config)# do show run | begin line
line con 0
password 7 04505F4E5E2741631A2A5454
login
line aux 0
no exec
login
password 7 075E36781F291C0627405C
line vty 0 4
password 7 065E18151D040C3E354232
login
!
end

User Authentication with AAA

Example 6-2 shows the use of method lists, both named and default.

**Example 6-2  Enabling AAA Services and Working with Method Lists**

R1(config)# aaa new-model

R1(config)# tacacs-server host 50.50.4.101
R1(config)# tacacs-server key ToUgHPaSsW0rD-1#7

! configure the default method list for the authentication of character mode login (where the user will have access to the CLI)
! This default method list, created below has two methods listed "local" and "enable"
This list is specifying that the local database (running-config) will be used first to look for the username. If the username isn't in the running-config, then it will go to the second method in the list. The second method of "enable" says that if the user account isn't found in the running config, then to use the enable secret to login. This default list will apply to all SSH, Telnet, VTY, AUX and Console sessions unless there is another (different) custom method list that is created and directly applied to one of those lines.

R1(config)# aaa authentication login default local enable

The next authentication method list is a custom authentication method list named MY-LIST-1. This method list says that the first attempt to verify the user's name and password should be done through one of the tacacs servers (we have only configured one so far), and then if that server doesn't respond, use the local database (running-config), and if the username isn't in the running configuration to then use the enable secret for access to the device. Note: this method list is not used until applied to a line elsewhere in the configuration.

R1(config)# aaa authentication login MY-LIST-1 group tacacs local enable

These next method lists are authorization method lists. We could create a default one as well, using the key word "default" instead of a name. These custom method lists for authorization won't be used until we apply them elsewhere in the configuration, such as on a VTY line. The first method list called TAC1 is an authorization method list for all commands at user mode (called privilege level 1). The second method list called TAC15 is an authorization method list for commands at level 15 (privileged exec mode). If these method lists are applied to a line, such as the console or VTY lines, then before any commands are executed at user or privileged mode, the router will check with an ACS server that is one of the "tacacs+" servers, to see if the user is authorized to execute the command. If a tacacs+ server isn't reachable, then the router will use its own database of users (the local database) to determine if the user trying to issue the command is at a high enough privilege level to execute the command.

R1(config)# aaa authorization commands 1 TAC1 group tacacs+ local
R1(config)# aaa authorization commands 15 TAC15 group tacacs+ local
The next 2 method lists are accounting method lists that will record the
commands issued at level 1 and 15 if the lists are applied to a line, and
if an administrator connects to this device via that line.
Accounting method lists can have multiple methods, but can't log to the
local router.

R1(config)# aaa accounting commands 1 TAC-act1 start-stop group tacacs+
R1(config)# aaa accounting commands 15 TAC-act15 start-stop group tacacs+

Creating a user with level 15 access on the local router is a good idea,
in the event the ACS server can't be
reached, and a backup method has been specified as the local database.
R1(config)# username admin privilege 15 secret 4Je7*1swEsf

Applying the named method lists is what puts them in motion.
By applying the method lists to the VTY lines
any users connecting to these lines will be authenticated by the
methods specified by the lists that are applied
and also accounting will occur, based on the lists that are applied.
R1(config)# line vty 0 4
R1(config-line)# login authentication MY-LIST-1
R1(config-line)# authorization commands 1 TAC1
R1(config-line)# authorization commands 15 TAC15
R1(config-line)# accounting commands 1 TAC-act1
R1(config-line)# accounting commands 15 TAC-act15

Note: on the console and AUX ports, the default list will be applied,
due to no custom method list being applied
directly to the console or AUX ports.

Using debug as a tool to verify what you think is happening is a good idea. In Example
6-3, we review and apply AAA and perform a debug verification.

Example 6-3  Another Example of Creating and Applying a Custom Method List to vty Lines

Creating the method list, which has 3 methods. First the local database
(if the username exists in the configuration, and if not
then the enable secret (if configured), and if not then no
authentication required
(no)
R2(config)# aaa authentication login MY-AUTHEN-LIST-1 local enable none

Applying the method list to the VTY lines 0-4
R2(config)# line vty 0 4
R2(config-line)# login authentication MY-AUTHEN-LIST-1
R2(config-line)# exit
Creating a local username in the local database (running-config)
R2(config)# username bob secret ciscobob

Setting the password required to move from user mode to privileged mode
R2(config)# enable secret ciscoenable
R2(config)# interface loopback 0

Applying an IP address to test a local telnet to this same local router
Not needed if the device has another local IP address that is in use
R2(config-if)# ip address 2.2.2.2 255.255.255.0
R2(config-if)# exit

Enable logging so we can see results of the upcoming debug
R2(config)# logging buffered 7
R2(config)# end

Enabling debug of aaa authentication, so we can see what the router is
thinking regarding aaa authentication
R2# debug aaa authentication
AAA Authentication debugging is on

R2# clear log
Clear logging buffer [confirm]

Telnet to our own address
R2# telnet 2.2.2.2
Trying 2.2.2.2 ... Open

User Access Verification

Username: bob
AAA/BIND (00000063): Bind i/f
AAA/AUTHEN/LOGIN (00000063): Pick method list 'MY-AUTHEN-LIST-1'
Password: [ciscobob] password not shown when typing it in

We can see that bob is connected via line vty 0, and that from the debug
the correct authentication list was used.

R2>who
Line       User       Host(s)              Idle       Location
0 con 0                2.2.2.2              00:00:00
* 2 vty 0     bob        idle                 00:00:00 2.2.2.2
R2> exit
If we exit back out, and remove all the users in the local database, (including bob) then the same login authentication will fail on the first method of the "local" database (no users there), and will go to the second method in the list, which is "enable", meaning use the enable secret if configured.

As soon as I supply a username, the router discovers that there are no usernames configured in running configuration (at least none that match the user who is trying to login), and fails on the first method "local" in the list. It then tries the next method of just caring about the enable secret.

```
R2# telnet 2.2.2.2
Trying 2.2.2.2 ... Open
User Access Verification

AAA/BIND(00000067): Bind i/f
AAA/AUTHEN/LOGIN (00000067): Pick method list 'MY-AUTHEN-LIST-1'

Note: bertha in not a configured user in the local database on the router
Username: bertha
Password: [ciscoenable] not shown while typing. This is the enable secret we set.
AAA/AUTHEN/ENABLE(00000067): Processing request action LOGIN
AAA/AUTHEN/ENABLE(00000067): Done status GET_PASSWORD

R2>
AAA/AUTHEN/ENABLE(00000067): Processing request action LOGIN
AAA/AUTHEN/ENABLE(00000067): Done status PASS
R2> exit

One more method exists in the method list we applied to the VTY lines. If the local fails, and the enable secret fails (because neither of these is configured on the router, then the third method in the method list 'MY-AUTHEN-LIST-1' will be tried. The third method we specified is none, meaning no authentication required, come right in. After removing the enable secret, we try once more.

R2# telnet 2.2.2.2
Trying 2.2.2.2 ... Open
User Access Verification
Using the CLI to Troubleshoot AAA for Cisco Routers

One tool you can use when troubleshooting AAA on Cisco routers is the debug command. You may use three separate debug commands to troubleshoot the various aspects of AAA:

- **debug aaa authentication**: Use this command to display debugging messages for the authentication functions of AAA.
- **debug aaa authorization**: Use this command to display debugging messages for the authorization functions of AAA.
- **debug aaa accounting**: Use this command to display debugging messages for the accounting functions of AAA.

Each of these commands is executed from privileged EXEC mode. To disable debugging for any of these functions, use the no form of the command, such as `no debug aaa authentication`.

Example 6-4 shows an example of debugging login authentication, EXEC authorization, and commands at level 15 authorization. As shown in the example, you can use `debug` not only for verification, as in the preceding example, but also as a troubleshooting method.

**Example 6-4  Using debug Commands**

```
! R4 will have a loopback, so we can telnet to ourselves to test
R4(config-if)# ip address 4.4.4.4 255.255.255.0
R4(config-if)# exit

! Local user in the database has a privilege level of 15
R4(config)# username admin privilege 15 secret cisco
```
! This method list, if applied to a line, will specify local authentication
R4(config)# aaa authentication login AUTHEN_Loc local

! This next method list, if applied to a line, will require authorization
! before giving the administrator an exec shell. If the user has a valid
! account in the running configuration, the exec shell will be created for
! the authenticated
! user, and it will place the user in their privilege level automatically
R4(config)# aaa authorization exec AUTHOR_Exec_Loc local

! This method list, if applied to a line, will require authorization for
! each and every level 15 command issued. Because the user is at
! privilege level 15 the router will say "yes" to any level 15 commands
! that may be issued by the user
R4(config)# aaa authorization commands 15 AUTHOR_Com_15 local

! Next we will apply the 3 custom method lists to vty lines 0-4, so that
! when anyone connects via these vty lines, they will be subject to the
! login authentication, the exec authorization, and the level 15 command
! authorizations for the duration of their session.

R4(config)# line vty 0 4
R4(config-line)# login authentication AUTHEN_Loc
R4(config-line)# authorization exec AUTHOR_Exec_Loc
R4(config-line)# authorization commands 15 AUTHOR_Com_15
R4(config-line)# exit
R4(config)#
R4(config)# do debug aaa authentication
AAA Authentication debugging is on
R4(config)# do debug aaa authorization
AAA Authorization debugging is on
R4(config)# exit

! Now test to see it all in action.
R4# telnet 4.4.4.4
Trying 4.4.4.4 ... Open
User Access Verification

Username: admin
Password: [cisco] password not displayed when entering

! It picked the login authentication list we specified
AAA/BIND(00000071): Bind i/f
AAA/AUTHEN/LOGIN (00000071): Pick method list 'AUTHEN_Loc'
Chapter 6: Securing the Management Plane on Cisco IOS Devices

! It picked the authorization list we specified for the exec shell
R4#
AAA/AUTHOR (0x71): Pick method list 'AUTHOR_Exec_Loc'
AAA/AUTHOR/EXEC (00000071): processing AV cmd=
AAA/AUTHOR/EXEC (00000071): processing AV priv-lvl=15
AAA/AUTHOR/EXEC (00000071): Authorization successful

! It picked the command level 15 authorization list, when we issued the
! configure terminal command, which is a level 15 command.
R4# config t
Enter configuration commands, one per line.  End with CNTL/Z.
R4(config)#
AAA/AUTHOR: auth_need : user= 'admin' ruser= 'R4' rem_addr= '4.4.4.4' priv=15 list='AUTHOR_Com_15' AUTHOR-TYPE= 'command'
AAA: parse name=ttty2 idb type=1 tty=-1
AAA: name=ttty2 flags=0x11 type=5 shelf=0 slot=0 adapter=0 port=2 channel=0
AAA/MEMORY: create_user (0x6A761F34) user='admin' ruser='R4' ds0=0 port='tty2'
rem_addr='4.4.4.4' authen_type=ASCII service=NONE priv=15 initial_task_id='0',
vrfl= (id=0)
tty2 AAA/AUTHOR/CMD (1643140100): Port='tty2' list='AUTHOR_Com_15'
service=CMD
AAA/AUTHOR/CMD: tty2(1643140100) user='admin'
tty2 AAA/AUTHOR/CMD (1643140100): send AV service=shell
tty2 AAA/AUTHOR/CMD (1643140100): send AV cmd=configure
tty2 AAA/AUTHOR/CMD (1643140100): send AV cmd-arg=terminal
tty2 AAA/AUTHOR/CMD (1643140100): send AV cmd-arg=<cr>
tty2 AAA/AUTHOR/CMD (1643140100): found list "AUTHOR_Com_15"
tty2 AAA/AUTHOR/CMD (1643140100): Method=LOCAL
AAA/AUTHOR (1643140100): Post authorization status = PASS_ADD
AAA/MEMORY: free_user (0x6A761F34) user='admin' ruser='R4' port='tty2'
rem_addr='4.4.4.4' authen_type=ASCII service=NONE priv=15 vrf= (id=0)
R4(config)#

! It made a big splash, with lots of debug output, but when you boil it all
! down it means the user was authorized to issue the configure terminal
! command.

There is also a test aaa command that is very useful when verifying connectivity with a
remote ACS server.

This section walked you through the details of AAA using the command line with very
exact examples because you need to understand how it works. Now that you have taken
a look at how it works, you should know that you can also use CCP as a GUI to implement the AAA.

Let's take a moment to review where you can find the AAA elements inside CCP. In the configuration section, using the navigation pane on the left, go to Configure > Router > AAA > AAA Summary. You will see there an overview of what authentication policies have been created on a router and any authorization or accounting policies, as shown in Figure 6-1.

![Figure 6-1 Using CPP to View AAA Policies](image)

If you wanted to add, edit, or modify your authentication policies, you just navigate to Configure > Router > AAA > Authentication Policies > Login, as shown in Figure 6-2.
If you want to see which method lists were applied to your vty lines, just navigate to Configure > Router > Router Access > VTY, as shown in Figure 6-3.

---

**Figure 6-2**  Using CCP to See Method Lists for Login

**Figure 6-3**  Using CCP to See Which Methods Have Been Applied to the vty Lines
From here, you can also modify which AAA policies are applied to vty lines by clicking Edit, which prompts the opening of an Edit VTY Lines dialog, as shown in Figure 6-4.

**Figure 6-4 Using CPP to Edit vty Line Properties, Including AAA Method Lists Applied**

**RBAC Privilege Level/Parser View**

You may implement RBAC through AAA, with the rules configured on an ACS server, but you may implement it in other ways, too, including creating custom privilege levels and having users enter those custom levels where they have a limited set of permissions, or creating a parser view (also sometimes simply called a view), which also limits what the user can see or do on the Cisco device. Each option can be tied directly to a user-name, so that once users authenticate they may be placed at the custom privilege level, or in the view that is assigned to them.

Let's implement a custom privilege level first, as shown in Example 6-5. The example includes explanations throughout.

**Example 6-5 Creating and Assigning Commands to a Custom Privilege Level**

```plaintext
! By default, we use privilege level 1 (called user mode), and privilege level 15 (called privileged mode). By creating custom levels, (between 1-15) and assigning commands to those levels, we are creating custom privilege levels
! A user connected at level 8, would have any of the new commands
! associated with level 8, as well as any commands that have been custom assigned or defaulted to levels 8 and below. A user at level 15 has access to all commands at level 15 and below.
```
Chapter 6: Securing the Management Plane on Cisco IOS Devices

This configuration assigns the command "configure terminal" to privilege level 8.

R2(config)# privilege exec level 8 configure terminal

This configuration command assigns the password for privilege level 8. The keyword "password" could be used instead of secret, but is less secure as the "password" doesn't use the MD5 hash to protect the password. The "0" before the password, implies that we are inputting a non-hashed (to begin with) password. The system will hash this for us, because we used the enable "secret" keyword.

R2(config)# enable secret level 8 0 NewPa5s123&
R2(config)# end

%SYS-5-CONFIG_I: Configured from console by console

To enter this level, use the enable command, followed by the level you want to enter. If no level is specified, the default level is 15.

R2# disable

Validate that user mode is really privilege level 1.

R2> show privilege
Current privilege level is 1

Context sensitive help shows that we can enter a level number after the word enable.

R2> enable ?
<0-15>  Enable level
view    Set into the existing view
<cr>

R2> enable 8
Password: [NewPa5s123&] ! note: password doesn't show when typing it in

R2> show privilege
Current privilege level is 8

We can go into configuration mode, because "configure terminal" is at our level.

R2# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

Notice we don't have further ability to configure the router, because level 8 doesn't include the interface configuration or other router configuration commands.

R2(config)# ?

Configure commands:
beep    Configure BEEP (Blocks Extensible Exchange Protocol)
call    Configure Call parameters
default Set a command to its defaults
If we are requiring login authentication, we can associate a privilege level with a given user account, and then when users authenticate with their username and password they will automatically be placed into their appropriate privilege level. Example 6-6 shows an example of this.

**Example 6-6  Creating a Local User and Associating That User with Privilege Level 8 and Assigning Login Requirements on the vty Lines**

```
! Create the user account in the local database (running-config) and ! associate that user with the privilege level you want that user to use.
R2(config)# username Bob privilege 8 secret Cisco123
R2(config)# line vty 0 4

! "login local" will require a username and password for access if the "aaa ! new-model" command is not present. If we have set the aaa new-model, ! then we would also want to create a default or named method list that ! specifies we want to use the local database for authentication.
R2(config-line)# login local

! Note: Once bob logs in, he would have access to privilege level 8 and ! below, (including all the normal show commands at level 1)
```

**Implementing Parser Views**

To restrict users without having to create custom privilege levels, you can use a parser view, also referred to as simply a view. A view can be created with a subset of privilege level 15 commands, and when the user logs in using this view, that same user is restricted to only being able to use the commands that are part of his current view.

To create a view, an enable secret password must first be configured on the router. AAA must also be enabled on the router (**aaa new-model** command).

Example 6-7 shows the creation of a view.
Example 6-7  Creating and Working with Parser Views

```
! Set the enable secret, and enable aaa new-model (unless already in
! place)
R2(config)# enable secret aBc!2#&iU
R2(config)# aaa new-model
R2(config)# end

! Begin the view creation process by entering the "default" view, using the
! enable secret
R2# enable view
Password: [aBc!2#&iU] note password not shown when typed

R2#
%PARSER-6-VIEW_SWITCH: successfully set to view 'root'.
R2# configure terminal

! As the administrator in the root view, create a new custom view
R2(config)# parser view New_VIEW
%PARSER-6-VIEW_CREATED: view 'New_VIEW' successfully created.

! Set the password required to enter this new view
R2(config-view)# secret New_VIEW_PW

! Specify which commands you want to include as part of this view.
! commands "exec" refer to commands issued from the command prompt
! commands "configure" refer to commands issued from privileged mode
R2(config-view)# commands exec include ping
R2(config-view)# commands exec include all show
R2(config-view)# commands configure include configure

! This next line adds the ability to configure "access-lists" but nothing
! else
R2(config-view)# commands configure include access-list
R2(config-view)# exit
R2(config)# exit

! Test the view, by going to user mode, and then back in using the new view
R2# disable
R2>enable view New_VIEW
Password: [New_VIEW_PW] Password not shown when typed in

! Console message tells us that we are using the view
%PARSER-6-VIEW_SWITCH: successfully set to view 'New_VIEW'.
```
! This command reports what view we are currently using
R2# show parser view
Current view is 'New_VIEW'

! We can verify that the commands assigned to the view work
! Note: we only assigned configure, not configure terminal so we have to
! use the configure command, and then tell the router we are configuring
! from the terminal. We could have assigned the view "configure terminal"
! to avoid this
R2# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

! Notice that the only configuration options we have are for access-list,
! per the view
R2(config)# ?
Configure commands:
  access-list  Add an access list entry
  do           To run exec commands in config mode
  exit        Exit from configure mode

We could also assign this view to a user account, so that when users log in with their
username and password, they are automatically placed into their view, as shown in
Example 6-8.

**Example 6-8  Associating a User Account with a Parser View**

R2(config)# username Lois view New_VIEW secret cisco123

**Note**  This creation of a username and assigning that user to a view needs to be done by
someone who is at privilege level 15.

**SSH and HTTPS**

Because Telnet sends all of its packets as plain text, it is not secure. SSH allows remote
management of a Cisco router or switch, but unlike Telnet, SSH encrypts the contents of
the packets to protect it from being interpreted if they fall into the wrong hands.

To enable SSH on a router or switch, the following items need to be in place:

- Hostname other than the default name of “router”
- Domain name
- Generating a public/private key pair, used behind the scenes by SSH
- Requiring user login via the vty lines, instead of just a password. Local authentication
  or authentication using an ACS server are both options.
Having at least one user account to log in with, either locally on the router, or on an ACS server.

Example 6-9 shows how to implement these components, along with annotations and examples of what happens when the required parts are not in place. If you have a non-production router or switch handy, you might want to follow along.

**Example 6-9  Preparing for SSH**

| ! To create the Public/Private key pair used by SSH, we would issue the following command. Part of the key pair, will be the hostname and the domain name. |
| ! If these are not configured first, the crypto key generate command will tell you as shown in the next few lines. |
| Router(config)# crypto key generate rsa % Please define a hostname other than Router. |
| Router(config)# hostname R1 |
| R1(config)# crypto key generate rsa % Please define a domain-name first. |
| R1(config)# ip domain-name cisco.com |

Now with the host and domain name set, we can generate the key pair

R1(config)# crypto key generate rsa
The name for the keys will be: R1.cisco.com
Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.

Bigger is better with cryptography, and we get to choose the size for the modulus

The default is 512 on many systems, but you would want to choose 1024 or more to improve security. SSH has several flavors, with version 2 being more secure than version 1. To use version 2, you would need at least a 1024 size for the key pair

How many bits in the modulus [512]: 1024 % Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R1(config)#
%SSH-5-ENABLED: SSH 1.99 has been enabled
! Note the "1.99" is based on the specifications for SSH from RFC 4253
! which indicate that an SSH server may identify its version as 1.99 to identify that it is compatible with current and older versions of SSH.

Create a user in the local database

R1(config)# username Keith secret CkRk*ks
! Configure the vty lines to require user authentication
R1(config)# line vty 0 4
R1(config-line)# login local

! Alternatively, we could do the following for the requirement of user authentication
! This creates a method list which points to the local database, and then applies that list to the VTY lines
R1(config)# aaa new-model
R1(config)# aaa authentication login Keith-List-1 local
R1(config)# line vty 0 4
R1(config-line)# login authentication Keith-List-1

! To test this we could SSH to ourselves from the local machine, or from another router that has IP connectivity to this router.

R1# ssh ?
-c  Select encryption algorithm
-l  Log in using this user name
-m  Select HMAC algorithm
-o  Specify options
-p  Connect to this port
-v  Specify SSH Protocol Version
-vrf  Specify vrf name

WORD IP address or hostname of a remote system

! Note: one of our local IP addresses is 10.1.0.1
R1# ssh -l Keith 10.1.0.1

Password: <password for Keith goes here>

R1>
! to verify the current SSH session(s)
R1# show ssh

<table>
<thead>
<tr>
<th>Connection</th>
<th>Version</th>
<th>Mode</th>
<th>Encryption</th>
<th>Hmac</th>
<th>State</th>
<th>Username</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>2.0</td>
<td>IN</td>
<td>aes128-cbc</td>
<td>hmac-shal</td>
<td>Session started</td>
<td>Keith</td>
</tr>
<tr>
<td>0</td>
<td>2.0</td>
<td>OUT</td>
<td>aes128-cbc</td>
<td>hmac-shal</td>
<td>Session started</td>
<td>Keith</td>
</tr>
</tbody>
</table>

%No SSHv1 server connections running.
R1>
Perhaps you want to manage a router via HTTPS. If so, you can use CCP or a similar tool and implement HTTPS functionality, as shown in Example 6-10.

**Example 6-10  Preparing for HTTPS**

```
! Enable the SSL service on the local router. If it needs to generate
! keys for this feature, it will do so on its own in the background.
R1(config)# ip http secure-server

! Specify how you want users who connect via HTTPS to be authenticated
R1(config)# ip http authentication ?
  aaa  Use AAA access control methods
  enable Use enable passwords
  local Use local username and passwords

R1(config)# ip http authentication local

! If you are using the local database, make sure you have at least one user
! configured in the running-config so that you can login. To test, open
! a browser to HTTPS://a.b.c.d where a.b.c.d is the IP address on the
! router.
```

**Implementing Logging Features**

Logging is important as a tool for discovering events that are happening in the network and for troubleshooting. Correctly configuring logging so that you can collect and correlate events across multiple network devices is a critical component for a secure network.

**Configuring Syslog Support**

Example 6-11 shows a typical syslog message and how to control what information is included with the message.

**Example 6-11  Using Service Time Stamps with Syslog Events**

```
R4(config)# interface fa0/0
R4(config-if)# shut

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to down
R4(config-if)#

! If we add timestamps to the syslog messages, those timestamps can assist it
! correlating events that occurred on multiple devices
```
R4(config)# service timestamps log datetime
R4(config)# int fa0/0
R4(config-if)# no shutdown

! These syslog messages have the date of the event, the event (just after ! the %) a description, and also the level of the event. The first is 3, ! the second is 5 in the example shown
*Nov 22 12:08:13: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Nov 22 12:08:14: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

To configure logging, you just tell CCP what the IP address of your syslog server is and which level of logging you want to do to that IP address. As a reminder, level 7, also known as debug level, sends all syslog alerts at level 7 and lower. To configure logging, navigate to Configure > Router > Logging, as shown in Figure 6-5.

Figure 6-5 Viewing the Logging Configuration

To modify any of the logging settings, click the Edit button, as shown in Figure 6-6.
In Figure 6-6, we have configured level 7 logging (debugging level) to a syslog server at the IP address of 10.1.0.25, and we have specified that the logging level to the buffer on the router is level 6 (informational level). The memory buffer to hold syslog messages is 8192 bytes. Beyond the 8192 bytes worth of messages in memory, any new messages will replace the oldest messages in a first in, first out (FIFO) manner. An example of a syslog server is syslog software running on a PC or dedicated server in your network.

The CCP (for the preceding scenario) creates the equivalent output at the CLI, as shown in Example 6-12.

**Example 6-12  CLI Equivalent Generated by CCP**

```
logging 10.1.0.25
logging trap debugging
logging buffered 8192 informational
```

Figure 6-7 shows the syslog output from the router being collected on the syslog server computer.
SNMP Features

Simple Network Management Protocol (SNMP) has become a de facto standard for network management protocols. The intent of SNMP is to manage network nodes, such as network servers, routers, switches, and so on. SNMP versions range from version 1 to 3, with some intermediate steps in between. The later the version, the more security features it has. Table 6-5 describes some of the components of SNMP.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP manager</td>
<td>An SNMP manager runs a network management application. This SNMP manager is sometimes called a Network Management Server (NMS).</td>
</tr>
<tr>
<td>SNMP agent</td>
<td>An SNMP agent is a piece of software that runs on a managed device (such as a server, router, or switch).</td>
</tr>
<tr>
<td>Management Information Base</td>
<td>Information about a managed device’s resources and activity is defined by a series of objects. The structure of these management objects is defined by a managed device’s Management Information Base (MIB). This can be thought of as a collection of unique numbers associated with each of the individual components of a router.</td>
</tr>
</tbody>
</table>

An SNMP manager can send information to, receive request information from, or receive unsolicited information (called a trap) from a managed device (a router). The managed device runs an SNMP agent and contains the MIB.
Even though multiple SNMP messages might be sent between an SNMP manager and a managed device, consider the three broad categories of SNMP message types:

- **GET**: An SNMP GET message is used to retrieve information from a managed device.
- **SET**: An SNMP SET message is used to set a variable in a managed device or to trigger an action on a managed device.
- **Trap**: An SNMP trap message is an unsolicited message sent from a managed device to an SNMP manager. It can be used to notify the SNMP manager about a significant event that occurred on the managed device.

Unfortunately, the ability to get information from or send configuration information to a managed device poses a potential security vulnerability. Specifically, if an attacker introduces a rogue NMS into the network, the attacker's NMS might be able to gather information about network resources by polling the MIBs of managed devices. In addition, the attacker might launch an attack against the network by manipulating the configuration of managed devices by sending a series of SNMP SET messages.

Although SNMP does offer some security against such an attack, the security integrated with SNMPv1 and SNMPv2c is considered weak. Specifically, SNMPv1 and SNMPv2c use *community strings* to gain read-only access/read-write access to a managed device. You can think of a community string much like a password. Also, be aware that multiple SNMP-compliant devices on the market today have a default read-only community string of “public” and a default read-write community string of “private.”

The security weaknesses of SNMPv1 and SNMPv2c are addressed in SNMPv3. SNMPv3 uses the concept of a security model and a security level:

- **Security model**: A security model defines an approach for user and group authentications.
- **Security level**: A security level defines the type of security algorithm performed on SNMP packets. Three security levels are discussed here:
  - **noAuthNoPriv**: The noAuthNoPriv (no authentication, no privacy) security level uses community strings for authentication and does not use encryption to provide privacy.
  - **authNoPriv**: The authNoPriv (authentication, no privacy) security level provides authentication using *Hashed Message Authentication Code (HMAC)* with *message digest algorithm 5 (MD5)* or *Secure Hash Algorithm (SHA)*. However, no encryption is used.
  - **authPriv**: The authPriv (authentication, privacy) security level offers HMAC MD5, or SHA authentication and also provides privacy through encryption. Specifically, the encryption uses the *Cipher Block Chaining (CBC) Data Encryption Standard (DES)* (DES-56) algorithm.

As summarized in Table 6-6, SNMPv3 supports all three of the previously described security levels. Notice that SNMPv1 and SNMPv2 support only the noAuthNoPriv security level.
Through the use of the security algorithms, as shown in Table 6-6, SNMPv3 dramatically increases the security of network management traffic as compared to SNMPv1 and SNMPv2c. Specifically, SNMPv3 offers three primary security enhancements:

- **Integrity**: Using hashing algorithms, SNMPv3 can ensure that an SNMP message was not modified in transit.
- **Authentication**: Hashing allows SNMPv3 to validate the source of an SNMP message.
- **Encryption**: Using the CBC-DES (DES-56) encryption algorithm, SNMPv3 provides privacy for SNMP messages, making them unreadable by an attacker who might capture an SNMP packet.

To configure SNMP on the router is simple, especially with CCP. If you know the community strings to use, and the IP address of the SNMP manager, you can configure it on the router by navigating to **Configure > Router > SNMP** and from there use the **Edit** button to add, change, or remove any of the SNMP-related settings. CCP enables command-line editing through the Utilities menu, but currently the SNMP Properties window does not support the configuration of SNMPv3. You can configure the basic SNMPv1 information, as shown in Figure 6-8.
The command-line output for this GUI would look similar to that shown in Example 6-13.

Example 6-13  Output Created by CCP for Implementing SNMPv1

```
snmp-server location 10.1.0.26
snmp-server contact Bubba Jones
snmp-server community super-secret RW
snmp-server host 10.1.0.26 trap cisK0tRap*
```

Configuring NTP

Because time is such an important factor, you should use Network Time Protocol (NTP) to synchronize the time in the network so that events that generate messages and time stamps can be correlated. You can use CCP to implement the NTP in addition to using the CLI. Let’s take a look at both right now.

To configure the NTP, you first need to know what the IP address is of the NTP server you will be working with, and you also want to know what the authentication key is and the key ID. NTP authentication is not required to function, but is a good idea to ensure that the time is not modified because of a rogue NTP server sending inaccurate NTP messages using a spoofed source IP address.

Armed with the NTP server information, in CCP you go to Configure > Router > Time > NTP and SNTP and click Add and put in the information about the server you will be getting the time from. When done, you click OK to close the dialog box. It may take anywhere between 5 and 15 minutes for the router to synchronize its clock. In Figure 6-9, this router is being told that the NTP server is at 55.1.2.3, that it should source the NTP requests from its IP address on its local Fast Ethernet 0/0 interface, and that it should use key number 1, and the password associated with that key. If multiple NTP servers were configured, the Prefer option is used to identify the preference of which NTP server to use.

Figure 6-9  Configuring a Router to Use an NTP Server
NTP supports authentication on a Cisco router because the router supports NTPv3. Example 6-14 shows the effective equivalent syntax that is created and delivered to the router.

**Example 6-14 Using Authentication via Keys with NTPv3**

```
ntp update-calendar
ntp authentication-key 1 md5 pAs5w0rd!3@
ntp authenticate
ntp trusted-key 1
ntp server 55.1.2.3 key 1 source FastEthernet0/0 prefer
```

To verify the status on this router acting as a NTP client, you could use the commands from the CLI as shown in Example 6-15.

**Example 6-15 Verifying Synchronization from the NTP Client**

```
R2# show ntp status
Clock is synchronized, stratum 4, reference is 55.1.2.3
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**24
reference time is D27619E3.7317ACB3 (12:53:55.449 UTC Tue Nov 22 2011)
clock offset is 0.0140 msec, root delay is 0.00 msec
root dispersion is 0.97 msec, peer dispersion is 0.43 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000000053 s/s
system poll interval is 64, last update was 130 sec ago.

R2# show ntp association
address ref clock st when poll reach delay offset disp
*~55.1.2.3 127.127.1.1 3 4 64 77 0.000 14.090 190.28
* sys.peer, # selected, + candidate, - outlyer, x falseticker,
~ configured
```

**Note** NTP uses UDP port 123. If NTP does not synchronize within 15 minutes, you may want to verify that connectivity exists between this router and the NTP server that it is communicating to. You also want to verify that the key ID and password for NTP authentication are correct.
Securing the Cisco IOS Image and Configuration Files

If a router has been compromised, and the flash file system and NVRAM have been deleted, there could be significant downtime as the files are put back in place before restoring normal router functionality. The Cisco Resilient Configuration feature is intended to improve the recovery time by making a secure working copy of the IOS image and startup configuration files (which are referred to as the primary bootset) that cannot be deleted by a remote user.

To enable and save the primary bootset to a secure archive in persistent storage, follow Example 6-16.

Example 6-16  Creating a Secure Bootset

```plaintext
! Secure the IOS image
R6(config)# secure boot-image
%IOS_RESILIENCE-5-IMAGE_RESIL_ACTIVE: Successfully secured running image

! Secure the startup-config
R6(config)# secure boot-config
%IOS_RESILIENCE-5-CONFIG_RESIL_ACTIVE: Successfully secured config archive
[flash:.runcfg-20111222-230018.ar]

! Verify the bootset
R6(config)# do show secure bootset
IOS resilience router id FTX1036A13J

IOS image resilience version 12.4 activated at 23:00:10 UTC Thu Dec 22 2011
Secure archive flash:c3825-advipservicesk9-mz.124-24.T.bin type is image
(elf) []
  file size is 60303612 bytes, run size is 60469256 bytes
  Runnable image, entry point 0x80010000, run from ram

IOS configuration resilience version 12.4 activated at 23:00:18 UTC Thu Dec 22 2011
Secure archive flash:.runcfg-20111222-230018.ar type is config
configuration archive size 1740 bytes

! Note: to undo this feature, (using the "no" option in front of the command)
! you must be connected via the console. This prevents remote users from
! disabling the feature.
```
Exam Preparation Tasks

Review All the Key Topics

Review the most important topics from this chapter, denoted with a Key Topic icon. Table 6-7 lists these key topics.

<table>
<thead>
<tr>
<th>Key Topic Element</th>
<th>Description</th>
<th>Page Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Text</td>
<td>Management plane best practices</td>
<td>95</td>
</tr>
<tr>
<td>Text</td>
<td>AAA components</td>
<td>98</td>
</tr>
<tr>
<td>Text</td>
<td>Storing usernames, passwords, and access rules</td>
<td>98</td>
</tr>
<tr>
<td>Text</td>
<td>Router access authentication</td>
<td>100</td>
</tr>
<tr>
<td>Table 6-2</td>
<td>AAA components to secure administrative and remote LAN access</td>
<td>101</td>
</tr>
<tr>
<td>Text</td>
<td>The AAA method list</td>
<td>101</td>
</tr>
<tr>
<td>Table 6-3</td>
<td>Method list options</td>
<td>101</td>
</tr>
<tr>
<td>Text</td>
<td>Limiting the administrator by assigning a view</td>
<td>103</td>
</tr>
<tr>
<td>Text</td>
<td>Encrypted management protocols</td>
<td>103</td>
</tr>
<tr>
<td>Text</td>
<td>Using logging files</td>
<td>104</td>
</tr>
<tr>
<td>Text</td>
<td>User authentication in AAA</td>
<td>108</td>
</tr>
<tr>
<td>Text</td>
<td>Using the CLI to troubleshoot AAA for Cisco routers</td>
<td>113</td>
</tr>
<tr>
<td>Example 6-4</td>
<td>Using debug commands</td>
<td>113</td>
</tr>
<tr>
<td>Example 6-5</td>
<td>Creating and assigning commands to custom privilege levels</td>
<td>118</td>
</tr>
<tr>
<td>Text</td>
<td>Implementing parser views</td>
<td>120</td>
</tr>
<tr>
<td>Example 6-7</td>
<td>Creating and working with parser views</td>
<td>121</td>
</tr>
<tr>
<td>Example 6-9</td>
<td>Preparing for SSH</td>
<td>123</td>
</tr>
<tr>
<td>Text</td>
<td>SNMP features</td>
<td>128</td>
</tr>
<tr>
<td>Table 6-6</td>
<td>Security models and security levels supported by Cisco IOS</td>
<td>130</td>
</tr>
<tr>
<td>Example 6-16</td>
<td>Creating a secure bootset</td>
<td>133</td>
</tr>
</tbody>
</table>
Complete the Tables and Lists from Memory

Print a copy of Appendix C, “Memory Tables,” (found on the CD) or at least the section for this chapter, and complete the tables and lists from memory. Appendix D, “Memory Tables Answer Key,” also on the CD, includes completed tables and lists so that you can check your work.

Define Key Terms

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

AAA, method list, custom privilege level, parser view, SSH, syslog, SNMP, NTP, secure bootset

Command Reference to Check Your Memory

This section includes the most important configuration and EXEC commands covered in this chapter. To see how well you have memorized the commands as a side effect of your other studies, cover the left side of Table 6-8 with a piece of paper, read the descriptions on the right side, and see whether you remember the commands.

Table 6-8  Command Reference

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>service password-encryption</td>
<td>Encrypt most plaintext passwords in the configuration.</td>
</tr>
<tr>
<td>aaa new-model</td>
<td>Enable AAA features.</td>
</tr>
<tr>
<td>aaa authentication login</td>
<td>Create a default method list for character mode login that will use the local database (running config) on the router or switch.</td>
</tr>
<tr>
<td>default local</td>
<td></td>
</tr>
<tr>
<td>enable view</td>
<td>Enter the root parser view, from where you can create additional views. This requires that aaa new-model already be in place in the configuration.</td>
</tr>
<tr>
<td>privilege exec level 8 show</td>
<td>Assign a show startup-config command to a custom privilege level 8.</td>
</tr>
<tr>
<td>startup-config</td>
<td></td>
</tr>
<tr>
<td>crypto key generate rsa</td>
<td>Create the public/private key pair required for SSH.</td>
</tr>
<tr>
<td>secure boot-image</td>
<td>Secure the IOS image on flash.</td>
</tr>
<tr>
<td>aaa authentication bubba</td>
<td>Create an authentication method list called bubba that will use the local database first, and if the username does not exist, will require the enable secret to allow login.</td>
</tr>
<tr>
<td>local enable</td>
<td></td>
</tr>
<tr>
<td>line console 0</td>
<td>Apply the method list named bubba to the console port.</td>
</tr>
<tr>
<td>login authentication bubba</td>
<td></td>
</tr>
</tbody>
</table>
### Index

**A**

<table>
<thead>
<tr>
<th>AAA (Authentication, Authorization, Accounting), 55</th>
</tr>
</thead>
<tbody>
<tr>
<td>accounting/auditing, 98</td>
</tr>
<tr>
<td>ACS</td>
</tr>
<tr>
<td>benefits, 140</td>
</tr>
<tr>
<td>configuring, 154-164</td>
</tr>
<tr>
<td>ISE, compared, 141</td>
</tr>
<tr>
<td>platforms supported, 141</td>
</tr>
<tr>
<td>router communication protocols, 141-143</td>
</tr>
<tr>
<td>routers, configuring, 142-154</td>
</tr>
<tr>
<td>troubleshooting, 164-170</td>
</tr>
<tr>
<td>AnyConnect SSL VPNs, 547-548</td>
</tr>
<tr>
<td>ASA support, 230, 333</td>
</tr>
<tr>
<td>authentication, 98</td>
</tr>
<tr>
<td>authorization, 98</td>
</tr>
<tr>
<td>best practices, 97-98</td>
</tr>
<tr>
<td>connectivity, testing, 115</td>
</tr>
<tr>
<td>enabling, 87</td>
</tr>
<tr>
<td>implementing</td>
</tr>
<tr>
<td>CCP, 116-118</td>
</tr>
<tr>
<td>command line, 113-115</td>
</tr>
<tr>
<td>IPv6, 211</td>
</tr>
<tr>
<td>management plane, 55</td>
</tr>
<tr>
<td>method lists, creating, 101-102</td>
</tr>
<tr>
<td>revoked certificates, 452</td>
</tr>
<tr>
<td>routers, 229</td>
</tr>
<tr>
<td>access authentication, 100</td>
</tr>
<tr>
<td>router-to-ACS, testing, 164-165</td>
</tr>
<tr>
<td>self-contained, 99</td>
</tr>
<tr>
<td>user authentication</td>
</tr>
<tr>
<td>best practices, 95</td>
</tr>
<tr>
<td>implementing, 108-113</td>
</tr>
<tr>
<td>usernames/passwords/access rules storage, 98-99</td>
</tr>
<tr>
<td>verifying, 146-147</td>
</tr>
<tr>
<td>VPN users, 99-100</td>
</tr>
<tr>
<td>access</td>
</tr>
<tr>
<td>AAA, 97-98</td>
</tr>
<tr>
<td>accounting/auditing, 98</td>
</tr>
<tr>
<td>authentication, 98</td>
</tr>
<tr>
<td>authorization, 98</td>
</tr>
<tr>
<td>method lists, creating, 101-102</td>
</tr>
<tr>
<td>router access authentication, 100</td>
</tr>
<tr>
<td>usernames/passwords/access rules storage, 98-99</td>
</tr>
<tr>
<td>VPN users, 99-100</td>
</tr>
<tr>
<td>ASA rules, 359-362</td>
</tr>
<tr>
<td>CBAC, 229</td>
</tr>
<tr>
<td>classes, HTTP service/vty lines, 87</td>
</tr>
<tr>
<td>controlling, 55-56</td>
</tr>
<tr>
<td>AAA services, 55</td>
</tr>
<tr>
<td>encrypted/authenticated SNMP, 56</td>
</tr>
<tr>
<td>IP addresses, 56</td>
</tr>
<tr>
<td>password policies, 55</td>
</tr>
</tbody>
</table>
RBAC, 55
syslog lockdown, 56
time accuracy, 56
firewall rules, 284
IPv6, controlling, 211
ports
assigning to VLANs, 178-179
negotiations, not allowing, 190
reflexive access lists, 229
remote-access VPNs, 427
role-based. See RBAC
rules, storing, 98-99
unauthorized, mitigating, 212
Access Control Entries (ACE), 243
access control lists. See ACLs
Access Control Server. See ACS
accounting (AAA), 98
accounts (user)
ACS, creating, 160
parser views, assigning, 122
ACE (Access Control Entries), 243
ACLs (Access Control Lists), 58
applying to interfaces, 249
ASA firewalls, 239
ASDM, 359-361
command line, 362
crypto, 481
data plane protection, 58
empty, 242
extended
defined, 242
identifying, 242
standard ACLs, compared, 243
IOS class maps, 239
IPv4 packet filtering
ACLs, creating, 246
applying ACLs to interfaces, 249
CLI implementation, 248
lines, adding, 246
object groups, 251-254
ordering, 247
policies, 244
rules, applying, 251
summary page (CCP), 245
verifying, 254
IPv6 packet filtering, 259-262
creating and applying, 261-262
ICMP, 262
objectives, 260
topology, 260
lines
adding, 246
numbers, 243
logging
firewall log details, 259
logs, viewing, 258
summary syslog messages, 257
syslog destinations, 258
malicious traffic
  general vulnerabilities, 241
  IP address spoofing, 240
  reconnaissance attacks, 240-241
  stopping, 239-240
  TCP SYN-flood attacks, 240
monitoring, 255-257
NAT/PAT, 239
object groups, 244
ordering, 247
outbound traffic, 242
packet-filtering, 239
  ASA firewalls, 230
  creating policies, 241
  enforcing policies, 241-242
  firewalls, 285
  routers, 229
QoS, 239
routing protocols, 239
standard
  defined, 242
  extended ACLs, compared, 243
  identifying, 242
traffic protection, classifying, 480-481
VPNs, 239
wildcard masks, 244
ACS (Access Control Server), 99
benefits, 140
configuring, 154-164
  adding network drives to device groups, 157-158
  authorization policies, 161-163
  device groups, creating, 156
  group summary, viewing, 159
  licensing, 156
  login screen, 156
  user accounts, creating, 160
  user groups, creating, 158
  functionality, 99
ISE (Identity Service Engine), 141
platforms supported, 141
routers, configuring, 142-154
  CCP, 148-154
  CLI, 144-147
  communication protocols, 141-143
  objectives, 142-144
self-contained AAA, 99
Solution Engine, 99
troubleshooting, 164-170
  AAA, 164-165
  connections, 164
  method lists, 166-170
  reports, 165-166
user authentication, 14
Windows, 99
actions
  IOS-based IPS response, 392
  policy maps, 296-297
  risk rating-based, implementing, 381
  signatures, 405
activating practice exams, 560
Adaptive Security Appliance (ASA)
  family models. See also ASA firewalls
Adaptive Security Device Manager.
  See ASDM
Address Resolution Protocol. See ARP
addresses
  bogus, filtering, 214
IP
  AnyConnect VPN clients,
    assigning, 548
  hosts, assigning, 203
  IKE Phase 2, planning, 501
  IPv6 versus IPv4, 203
  management sessions, controlling,
    56
  source interfaces, testing, 515-516
source NAT, 278-279
spoofing attacks, preventing, 240
IPv6
   all-nodes multicast, 206
   all-routers multicast addresses, 206
decimal/binary/hexadecimal conversions, 204
   formatting, 202-204
   hexadecimal hard way example, 204-205
IPv4, compared, 203
   link local, 205-206
loopback, 206
   multicast, 207
   remote device communication, 205
   solicited-node multicast, 207
   unicast/anycast, 206-207
   zero shortcuts, 205
link local, 205-206
loopback, 206
MAC
   flooding, 59
   port security, 192-194
   multicast, 207
   all-nodes, 206
   all-routers, 206
   non-local, filtering, 215
   solicited-node, 207
administrator
   access/protocols, protecting, 55-56
   AAA services, 55
   encrypted/authenticated SNMP, 56
   IP addresses, controlling, 56
   password policies, 55
   RBAC, 55
   syslog lockdown, 56
   time accuracy, 56
   control countermeasures, 12
alarm summarization (IOS-based IPS), 392
alerts
   details, viewing, 414
   IPS/IDS
      delivering, 385
      types, 380
   signatures, viewing, 413-414
   viewing
      command line, 415-416
      SDEE log file screen, 413-414
   all-nodes multicast addresses, 206
   all-routers multicast addresses, 206
analysis
   cost-benefit, 9-10
   risks, 25-26
      current posture assessment, 26-27
      qualitative, 26
      quantitative, 26
anomaly-based IPS/IDS, 378
antireplay functionality
   IPsec support, 468-469
   VPN component, 430
anycast addresses, 206-207
AnyConnect Client, 42
   installing, 550
   software packages, choosing, 546-547
   SSL, AnyConnect connection profile/
      tunnel group/Group correlation, 553
AnyConnect SSL VPNs
   AnyConnect client
      installing, 550
      software packages, choosing, 546-547
   authentication, 547-548
   clientless SSL VPNs, compared, 545
   command line configuration, 550-552
connection profiles, creating, 545
digital certificates, 546
DNS, configuring, 548
domain name configurations, 548
groups, 552-553
IP address pool, assigning, 548
NAT exemptions, 549
overview, 534
protocols, choosing, 546
split tunneling, 554-555
SSL AnyConnect connection profile/
tunnel group/Group correlation, 553
summary page, 550
VPN AnyConnect Wizard, starting, 545
WINS, configuring, 548
application inspection firewalls, 276
application layer
attacks, 212
gateways
  firewalls, 275
inspections/awareness, 331-332
IPv6 versus IPv4, 203
visibility, 226
application policies, 30
applying
ACLs
  rules, 251
  interfaces, 249
ASA policies, 339-340
IPv6 ACLs as filters, 261-262
method lists (AAA), creating, 152
object groups, 253-254
templates (CCP), 76-77
user profiles (CCP), 80
AR (attack relevancy), 382
ARP (Address Resolution Protocol), 85
dynamic, 228
  gratuitous, 85
  proxy, 86
ASA family models, 330-331
ASA firewalls, 42
AAA support, 333
access rules, 359-362
ACLs, 239
AnyConnect software packages,
  choosing, 546-547
application inspection/awareness,
  331-332
ASDM. See ASDM
availability, 333
botnets, filtering, 333
client IP addresses, 355
clientless SSL VPNs
  authentication, 538-540
  CLI implementation, 540-541
  configuring, 535-544
digital certificates, 537
  interfaces, 537
logging in, 541-542
  session details, viewing, 543-544
SSL VPN Wizard, 535-544
configuring, 340-345
  initial boot, 340-343
  setup script, running, 343-345
connections
  console ports, 337
  verifying, 345
default traffic flow, 335-336
DHCP, 332
DMZ, 334
group objects, 333
interfaces
  configuring, 347-355
editing, 351
final configuration, 352
implementing, 352-355
maximum allowed, 350
summary page, 350
VLAN number associations, 349-350
Layer 2/Layer 3 implementations, 332
managing, 336-337
NAT, 332, 357-359
implementing, 357
verifying, 358
packet filtering, 331, 337-338
implementing, 338
inbound traffic, 337-338
outbound traffic, 338
Packet Tracer, 362-367
command line, 364-366
input, configuring, 332-362
launching, 362
results, 363-364
Telnet denial, verifying, 366-367
PAT, 357-359
dynamic, implementing, 358
rules verification, 358
policies
applying, 339-340
MPF, 338-339
routing, 332, 356-357
security features, 230
AAA, 230
ACLs (packet-filtering), 230
IPS, 230
management protocols, 230
MPF, 230
routing protocol authentication, 230
stateful filtering, 230
URL filtering, 230
VPNs, 230
security levels, 333-334
self-signed certificates, 454
split tunneling, 554-555
stateful filtering, 331
VPN support, 333
ASDM (Adaptive Security Device Manager)
ACLs, implementing, 359-361
certificates, viewing, 455
clientless SSL VPNS. See clientless SSL VPNS, configuring on ASA
dashboard, 345
interfaces
customizing, 347-355
editing, 351
final configuration, 352
implementing, 352-355
maximum allowed, 350
summary page, 350
VLAN number associations, 349-350
overview, 337
Packet Tracer, 362-367
input, configuring, 362
launching, 362
results, 363-364
running, 345-347
Startup wizard, 346-347
usernames/passwords/access rules storage, 345
ASR (attack severity rating), 382, 384-385
assets
classifying, 10-11
criteria, 11
governmental, 11
private sector, 11
roles, 11

assets  591
defined, 9-10
risk management, 27-28
asymmetric algorithms, 438
examples, 444
key length, 444
overview, 433
atomic micro-engine, 384
attack relevancy (AR), 382
attack severity rating (ASR), 382
attacks, 14-15
application layer, 212
back doors, 15
botnets, 17
CAM overflow, 59
covert channels, 17
dictionary, 85
DoS/DDoS, 17
IPv6, 211-212
preventing, 59
TCP SYN-flood attacks, 240
evidence, collecting, 32
incident response policies, 32
malicious traffic
general vulnerabilities, 241
IP address spoofing, 240
reconnaissance, 240-241
sensor responses, 379-380
stopping, 239-240
TCP SYN-flood attacks, 240
man-in-the-middle, 14-16, 212
packet amplification, 214
password, 17
potential attackers, 13-14
motivations/interests,
understanding, 14
types, 13
privilege escalation, 15
reconnaissance, 15
routers, 213
social engineering, 15
spoofing, preventing, 59
timing, 381
trust exploitation, 17
vectors, 14
auditing, 16
AAA, 98
CCP Security Audit, 81
AAA, enabling, 87
authentication failure rates, 85
banners, setting, 85
BOOTP service, disabling, 84
CDP, 84
CEF, enabling, 85
enable secret password, setting, 86
Finger service, disabling, 84
firewalls, enabling, 87
fixing identified potential problems, 82-83
gratuitous ARPs, 85
HTTP service/vty lines access class, setting, 87
ICMP redirects, disabling, 86
identification service, disabling, 84
identifying potential problems, 82
interface connections, 82
IP directed broadcasts, disabling, 87
IP mask reply messages, disabling, 87
IP source route, disabling, 85
IP unreachables, disabling, 87
logging, enabling, 85
minimum password lengths, 85
MOP, disabling, 87
One-Step Lockdown, 84
options, 81
password encryption, enabling, 85
proxy ARPs, disabling, 86
RPF, enabling, 87
scheduler allocation, 86
scheduler interval, setting, 86
SNMP, disabling, 86
SSH, 87
starting, 81
summary, 83
TCP keepalives, enabling, 85
TCP small servers service, disabling, 84
TCP SYN-Wait times, setting, 85
Telnet settings, enabling, 86
UDP small servers service, disabling, 84
users, configuring, 86
authentication
AAA, 98
ACS method lists
  routers, configuring, 144
testing, 166-170
AnyConnect SSL VPNs, 547-548
CAs (certificate authorities), 450
failure rates, setting, 85
IKE Phase 1
  peer, 471
  planning, 499
tunnel negotiations, 470
IPsec, 468-469, 499
method lists, 149-150
NTP, 132
routing protocols
  ASA firewalls, 230
ccontrol plane, 56
IPv6, 211
routers, 229
SNMPv3, 130
SSL VPN users, 538-540
  bookmarks provided, editing, 539
  groups, assigning, 538
  methods, 538
  summary page, 540
users
  best practices, 95
  implementing, 108-113
  requiring, 14
VPNs, 99-100, 430, 438
Authentication, Authorization, Accounting. See AAA
authNoPriv security level (SNMP), 129
authorization
AAA, 98
ACS method lists
  routers, configuring, 144, 150-151
testing, 166-170
ACS policies
  creating, 161-163
  customizing, 163
  profiles, 162
profiles, 162
VPN users, 99-100
authPriv security level (SNMP), 129
availability
ASA, 333
defined, 9
back doors, 15
bandwidth management, 59
banners, configuring, 85
B


Basic Firewall wizard
CME warning message, 303
DNS, choosing, 305
interfaces
  connecting, 302
  not belonging warning message, 303
  untrusted warning message, 303
security levels, choosing, 304
summary page, 305
welcome screen, 302
binary/decimal/hexadecimal conversions, 204
block ciphers, 432
BOOTP service, disabling, 84
borderless networks
  changing nature of networks, 40
data centers, 41
defined, 36
end zones, 41
Internet, 41
logical boundaries, 40-41
policy management points, 41
prevention strategies, 42-43
  ASA firewalls, 42
  IPS (Intrusion Prevention System), 43
  IronPort Email Security/Web Security Appliances, 43
  ISR (Integrated Services Routers), 42
  ScanSafe, 43
secured management protocols, 43
SecureX architecture, 42
  AnyConnect Client, 42
  context awareness, 42
  SIO (Security Intelligence Operations), 42
  TrustSec, 42
single-console management tools, 43
VPN connectivity, 43
botnets, 17, 333
BPDU (bridge protocol data units), 184
BPDU guards
  implementing, 190-191
  switches, 228
broadcasts (IP)
  directed, disabling, 87
  IPv6 versus IPv4, 203
buffer logs, receiving, 104
bugs (IPv6), 214
business continuity planning, 33
buttons (CCP toolbar), 68

C

C3PL (Cisco Common Classification Policy Language), 296
Call Manager Express (CME), 303
CAM (content-addressable memory)
  overflow attacks, 59
CAs (certificate authorities), 446
  authenticating, 450
  certificate information, 446
  commercial, 446
  cross-certifying, 453
  enrolling, 450
  hierarchical with subordinate CAs, 453
  IPsec site-to-site VPNs, 504-505
  overview, 460
  single root, 453
  subordinate CAs, 460
CBAC (Context-Based Access Control), 229
CCP (Cisco Configuration Professional), 63
AAA, implementing, 116-118
ACLS
applying to interfaces, 249
creating, 246
lines, adding, 246
object groups, creating, 251-252
ordering, 247
summary page, 245
alerts, viewing
IPS Alert Statistics tab, 414
IPS Signature Statistics tab, 413
SDEE log file screen, 413-414
benefits, 63
commands, previewing, 83
communities, 70-73
adding devices, 72-73
creating, 71
defined, 71
discovering devices, 73
maximum devices, 71
configuring routers for ACS servers, 148-154
ACS servers, adding, 148
applying method lists, 152
authentication method lists, 149-150
authorization method lists, 150-151
local users, adding, 153-154
method lists, creating, 149
Express, 65
IKE Phase 1, configuring, 506-507
IKE Phase 2, configuring, 507-508
interface
content pane, 69
left navigation pane, 67
menu bar, 66
status bar, 69
toolbar, 67-68
IOS-based IPS installation, 394-400
configuration screen navigation, 394
deployment bit on CPU resources, 398
interfaces, choosing, 396
IPS policy welcome page, 395
public key, adding, 397
router subscriptions, opening, 395
SDEE, enabling, 395
signature file locations, defining, 396-397
signatures, compiling, 399-400
summary page, 398
traffic inspection direction, 396
IPS signatures
configuration changes output, 403-404
editing, 401
enabling, 404-405
filtering based on signature IDs, 402
modification buttons, 401
properties, editing, 402
viewing, 400
IPsec, configuring, 475-484
IKE Phase 1 policy, 477-478
local Ethernet information, entering, 477
remote peer information, entering, 477
Step by Step wizard, 476
summary, 481
traffic encryption, 480-481
transform sets, 479-480
layout, 65
licensing, 65
logging
  configuring, 126
  editing, 126-127
NAT
  configuring, 319-321
  verifying, 322
NTP configuration, 131
overview, 65
router communication, configuring, 69-70
Security Audit, 81
  AAA, enabling, 87
  authentication failure rates, 85
  banners, setting, 85
  BOOTP service, disabling, 84
  CDP, disabling, 84
  CEF, enabling, 85
  enable secret password, setting, 86
  Finger service, disabling, 84
  firewalls, enabling, 87
  fixing identified potential problems, 82-83
  gratuitous ARPs, disabling, 85
  HTTP service/vty lines access class, setting, 87
  ICMP redirects, disabling, 86
  identification service, disabling, 84
  identifying potential problems, 82
  interface connections, 82
  IP directed broadcasts, disabling, 87
  IP mask reply messages, disabling, 87
  IP source route, disabling, 85
  IP unreachable, disabling, 87
  logging, enabling, 85
  minimum password lengths, 85
  MOP, disabling, 87
One-Step Lockdown, 84
  options, 81
  password encryption, enabling, 85
  proxy ARPs, disabling, 86
  RPF, enabling, 87
  scheduler allocation, setting, 86
  scheduler interval, setting, 86
  SNMP, disabling, 86
  SSH, enabling, 87
  starting, 81
  summary, 83
  TCP keepalives, enabling, 85
  TCP small servers service, disabling, 84
  TCP SYN-Wait times, setting, 85
  Telnet settings, enabling, 86
  UDP small servers service, disabling, 84
  users, configuring, 86
SNMP, configuring, 130-131
templates, 74-78
  applying, 76-77
  creating, 75-76
  merging/overriding options, 77-78
toolbar properties, 67
user profiles, 78-80
  applying, 80
  creating, 79
  restrictions, 78
  saving, 80
  verifying, 80
ZBFs, configuring, 300-313
  Basic Firewall wizard welcome screen, 302
  CME warning message, 303
  DNS, choosing, 305
  Firewall wizard page, 301-302
interface not belonging warning message, 303
interfaces, connecting, 302
literal CLI commands generated, 306-313
security levels, choosing, 304
summary page, 305
untrusted interfaces warning message, 303
verifying, 314-315
CD (book)
installing, 560
videos, 562
CDP (Cisco Discovery Protocol), 84
CEF (Cisco Express Forwarding), 85
central servers, 98-99
centralized authentication servers.
  See ACS
centralized monitoring, 226
Certificate Revocation Lists (CRLs), 452
certificates, 460
  AnyConnect SSL VPNs, 546
  ASA self-signed, 454
  authorities, 446
    authenticating, 450
    certificate information, 446
    commercial, 446
    cross-certifying, 453
    enrolling, 450
    hierarchical with subordinate CAs, 453
  IPsec site-to-site VPNs, 504-505
  overview, 460
  single root, 453
  subordinate CAs, 460
clientless SSL VPNs, 537
functions, 452
identity, 448
  installing with SCEP, 457-459
  manually installing, 456
  requesting, 450
IPsec site-to-site VPNs, 504-505
issuers, 449
peers public keys, obtaining, 448
public keys, 449
revocation list location, 449
revoked, 451-452
root, 446-448
  authenticating, 450
  installing with SCEP, 457-459
  issuers, 447
  manually installing, 455-456
  public keys, 448
  serial numbers, 447
  subjects, 447
  thumbprint, 448
  validity dates, 447
SCEP (Simple Certificate Enrollment Protocol), 451
serial numbers, 449
signatures, 449
subjects, 449
thumbprint, 449
validity dates, 449
viewing in ASDM, 455
X.500/X.509v3, 449, 460
challenges, 4
Change Default Credentials dialog box, 72
ciphers
asymmetrical, 433
block, 432
defined, 431
polyalphabetic, 431
stream, 432
substitutions, 431
symmetrical, 432-433
transposition, 431
Cisco Configuration Professional.
See CCP
Cisco Discovery Protocol (CDP), 84
Cisco Express Forwarding (CEF), 85
Cisco Learning Network, 561
Cisco Security Manager (CSM), 43, 231
class maps
ASAs, 339
defined, 296
classifying
assets, 10-11
criteria, 11
governmental, 11
private sector, 11
roles, 11
countermeasure controls, 12
administrative, 12
logical, 12
physical, 12
vulnerabilities, 11-12
clientless SSL VPNs
AnyConnect SSL VPNs, compared, 545
configuring on ASA, 535-544
authentication, 538-540
CLI implementation, 540-541
digital certificates, 537
interfaces, 537
SSL VPN Wizard, 535-544
logging in, 541
overview, 534
session details, viewing, 543-544
CME (Call Manager Express), 303
collecting evidence, 32
command line
ACLs
implementing, 248
monitoring, 255-257
object groups, creating, 253
alerts, viewing, 415-416
AnyConnect SSL VPNs, configuring, 550-552
ASA access rules, implementing, 362
CA authentication/enrollment, 458-459
clientless SSL VPNs implementation, 540-541
configuring routers for ACS servers, 144-147
AAA, verifying, 146-147
authentication method lists, 144
authorization method lists, 144
overview, 147
crypto policies, configuring, 509-510
IOS-based IPS
installing, 407-412
signature compilation output, 399-400
IPsec
configuring, 482-484
verifying, 486-490
logging, configuring, 126-127
NAT
configuring, 322
verifying, 323
Packet Tracer, 364-366
signature configuration changes output, 403-404
SNMP, configuring, 131
ZBFs
configuration commands, 306-313
verifying, 315-319
commands
AAA method lists, 102
CCP, previewing, 83
debug
   AAA, 113-115
   ACS method lists, 166-170
   IKE Phase 1, 512
ping
   IPsec traffic triggers, 512
   router-to-ACS connections, 164
   routers, 499
   signatures, 406
   source interfaces with associated
   IP addresses, 515-516
test aaa, 115, 164-165
commercial CAs, 446
Common Classification Policy Language
   (C3PL), 296
Common Vulnerabilities and Exposures
   (CVE) database, 12
communication. See also traffic
   ACS server to router protocols, 141-143
      choosing, 142-143
      RADIUS, 142
      TACACS+, 141
   CCP/routers, configuring, 69-70
encryption
   best practices, 95
   HTTPS, implementing, 125
   SSH, implementing, 122-124
communities, 70-73
   creating, 71
   defined, 71
devices
   adding, 72-73
   discovering, 73
   maximum, 71
companion website, 573
confidentiality
   defined, 8
   IPsec, 468, 499
   VPNs, 428, 438
Configure button (CCP toolbar), 68
configuring
   ACS, 154-164
      adding network drives to
      device groups, 157-158
      authorization policies, 161-163
      device groups, creating, 156
      group summary, viewing, 159
      licensing, 156
      login screen, 156
      user accounts, creating, 160
      user groups, creating, 158
ASAs, 340-345
   ASDM, 345-347
      initial boot, 340-345
      setup script, running, 343-345
authentication failure rates, 85
   banners, 85
CCC/router communication, 69-70
clientless SSL VPNs on ASA, 535-544
   authentication, 538-540
   CLI implementation, 540-541
   digital certificates, 537
   interfaces, 537
   SSL VPN Wizard, 535-544
crypto policies, 508-510
DNS for AnyConnect clients, 548
domain names for AnyConnect
   clients, 548
enable secret password, 86
firewall interfaces, 347-355
   final configuration, 352
   maximum allowed, 350
600 configuring

**Summary page, 350**

- VLAN number associations, 349-350
- HTTP service/vty lines access class, 87
- IKE Phase 1, 506-507
- IKE Phase 2, 507-510
- Interfaces, 351
- IPsec, 475-484
  - Command line, 482-484
  - IKE Phase 1 policy, 477-478
  - Local Ethernet information, entering, 477
- Mirrored VPN for remote peers, 485-486
- Remote peer information, entering, 477
- Step by Step wizard, 476
- Summary, 481
- Traffic encryption, 480-481
- Transform sets, 479-480
- VPN tunnel status, 484

- IPv6 routing, 208-210
- Logging, 126
- NAT, 281, 319-322
- NTP, 131-132, 502
  - Authentication, 132
  - CCP, 131
  - Synchronization, verifying, 132
- Packet Tracer input, 332-362
- Password lengths, 85
- Rapid Spanning Tree, 187-188
- Routers for ACS servers, 142-154
  - CCP, 148-154
  - CLI, 144-147
  - Objectives, 142-144
- Scheduler
  - Allocation, 86
  - Intervals, 86

**SNMP**

- CCP, 130-131
  - Command line, 131
- Split tunneling, 554
- Syslog support, 125-126
- TCP SYN-Wait times, 85
- Thresholds, 392
- Trunk ports, 180-181
- Users, 86
- WINS for AnyConnect clients, 548
- ZBF components, 298-300

**ZBFs, 300-313**

- Basic Firewall wizard welcome screen, 302
- CME warning message, 303
- DNS, choosing, 305
- Firewall wizard page, 301-302
- Interface not belonging warning message, 303
- Interfaces, connecting, 302
- Literal CLI commands, 306-313
- Security levels, choosing, 304
- Summary page, 305
- Untrusted interfaces warning message, 303

**Connections**

- AAA, testing, 115
- AnyConnect SSL VPNs profiles, creating, 545
- ASAs
  - Console ports, 337
  - Verifying, 345
- Clientless SSL VPNs logins, 541
- Interfaces (ZBF zones), 302
- Management plane, 94
- Router-to-ACS, testing, 164
- VPNs, 43
console logs, receiving, 104
content-addressable memory (CAM) attacks, 59
content pane (CCP), 69
context awareness, 42
Context-Based Access Control (CBAC), 229
control plane
CoPP, 56
CPPr, 56
defined, 52
nontransit traffic, 56
protection/policing, 229
routing protocol authentication, 56
security measures, 54
Control plane policing (CoPP), 56
Control plane protection (CPPr), 56
cost-benefit analysis, 9-10
countermeasures
classifying, 12
administrative controls, 12
logical controls, 12
physical controls, 12
defined, 9-10
designing
ACLs. See ACLs
application layer visibility, 226
ASA firewalls, 230
centralized monitoring, 226
CSM (Cisco Security Manager), 231
defense in depth, 226
end-user education, 226
end user risks, 224-225
incident responses, 226
IPS (Intrusion Prevention System), 231
mitigation policies/techniques, 226
opportunities for attacks, 224
policy procedures, 226
potential risks, 224
routers, 227-229
SIO services, 231
switches, 227
DoS attacks, 211
firewall risks
exposure of sensitive systems to untrusted individuals, 271
malicious data, 271
protocol flaw exploitation, 271
unauthorized users, 271
IPv6 threats
application layer attacks, 212
DoS attacks, 212
man-in-the-middle attacks, 212
router attacks, 213
sniffing/eavesdropping, 212
spoofed packets, 212
unauthorized access, 212
Layer 2 threats
best practices, 189
BPDU guards, 190-191
erd-disabled ports, restoring, 191-192
negotiations, not allowing, 190
port security, 192-194
root guards, 192
switch ports, locking down, 189-190
tools, 190
malicious traffic attacks, 379-380
deny attacker inline, 380
deny connection inline, 380
deny packet inline, 380
log attacker packets, 380
log pair packets, 380
log victim packets, 380
produce alert, 380
produce verbose alert, 380
request block connection, 380
request block host, 380
request SNMP trap, 380
threats
mitigation/containment strategies, designing, 224
covert channels, 17
CPPr (Control plane protection), 56
creating
AAA method lists, 101-102
ACS authorization policies, 161-163
customizing, 163
profiles, 162
AnyConnect SSL VPNs connection profiles, 545
device groups, 156
digital signatures, 445
firewall rules, 285-286
IPv6 ACLs, 261-262
key pairs, 457
object groups, 251-253
packet-filtering ACL policies, 241
parser views, 103, 121-122
passwords, 97
policies (security), 28
strategies
changing nature of networks, 40
logical boundaries, 40-41
prevention, 42-43
secured management protocols, 43
SecureX architecture, 42
single-console management tools, 43
VPN connectivity, 43
subinterfaces, 182-183
templates (CCP), 75-76
traffic tags, 180-181
transform sets, 479
users
accounts, 160
groups, 158
profiles, 79
CRLs (Certificate Revocation Lists), 452
cross-certifying CAs, 453
crypto ACLs, 481
crypto policies, configuring, 508-510
cryptography, 430
asymmetric, 438
ciphers
block, 432
defined, 431
polyalphabetic, 431
substitution, 431
transposition, 431
digital signatures, 438
creating, 445
DSA, 444
RSA, 460
VPN functions, 435-436
hashes, 434
data integrity, verifying, 434
HMAC (Hashed Message Authentication Code), 434
deny attacker inline sensor response

overview, 434
types, 434
keys, 431
  Diffie-Hellman key exchange, 438
  keyspace, 436
  lengths, 433
  managing, 436
  public key cryptography, 433
PKI. See PKI
stream ciphers, 432
symmetric, 432-433, 438
CSM (Cisco Security Manager), 43, 231
current posture assessment, 26-27
  external, 27
  general, 27
  internal, 27
  wireless, 27
custodians (asset classification), 11
customizing
  ACS authorization policies, 163
  firewall interfaces, 351
logging settings
  CCP, 126
  command line, 127
  privilege levels, 103, 118-120
  signatures, 401, 406
CVE (Common Vulnerabilities and Exposures) database, 12

data plane
  ACLs, 58
  bandwidth management, 59
  CAM overflow attacks, 59
  DAI, 59
  defined, 53
  DHCP snooping, 59
  DoS attacks, preventing, 59
  IOS
    firewall support, 58
    IPS, 58
  IP source guard, 59
  IPS (Intrusion Prevention System), 59
  MAC address flooding, 59
  security measures, 54
  spoofing attacks, preventing, 59
  TCP intercept, 58
  transit traffic, 56
  unicast reverse path forwarding, 58
  unwanted traffic, blocking, 59
databases, public domain threats, 12
DDoS (Distributed Denial-of-Service) attacks, 17. See also DoS
debug commands
  AAA, 113-115
  ACS method lists, 166-170
  IKE Phase 1, 512
decimal/binary/hexadecimal conversions, 204
default command (AAA method lists), 102
defense in depth, 16
  firewalls, 272-273
  threats, mitigating, 226
delivering IPS/IDS alerts, 385
Denial-of-Service attacks. See DoS
deny attacker inline sensor response, 380

DAI (Dynamic ARP inspection), 59
dashboard (ASDM), 345
data centers, 41
data integrity
  IPsec, 468, 499
  verifying, 434
  VPNs, 428-430, 438
deny connection inline sensor response, 380
deny packet inline sensor response, 380
deployment
  firewalls, 283-284
  NAT options, 281
designing threat mitigation/containment strategies, 224
  ASA firewalls, 230
    AAA, 230
    ACLs (packet-filtering), 230
    IPS (Intrusion Prevention System), 230
    management protocols, 230
    MPF, 230
    routing protocol authentication, 230
    stateful filtering, 230
    URL filtering, 230
    VPNs, 230
  components
    application layer visibility, 226
    centralized monitoring, 226
    defense in depth, 226
    end-user education, 226
    incident responses, 226
    mitigation policies/techniques, 226
    policy procedures, 226
  CSM (Cisco Security Manager), 231
  end user risks, 224-225
  IPS (Intrusion Prevention System), 231
  opportunities for attacks, 224
  potential risks, 224
  routers, 227-229
    AAA, 229
    ACLs (packet-filtering), 229
    CBAC, 229
control plane protection/policing, 229
  IPS, 229
  management protocols, 229
  reflexive access lists, 229
  routing protocol authentication, 229
  VPNs, 229
  Zone-Based Firewalls, 229
  SIO services, 231
  switches, 227
    BPDU guards, 228
    DHCP snooping, 228
    dynamic ARP inspections, 228
    IP source guards, 228
    modules, 228
    port security, 228
    root guards, 228
    storm control, 228
device groups, creating, 156-158
devices, hardening, 211
DHCP (Dynamic Host Configuration Protocol), 59
  ASA, 332, 355
  IPv6
    IPv4, compared, 203
    risks, 213
  snooping, 59, 228
dialog boxes
  Change Default Credentials, 72
  Manage Community, 71
dictionary attacks, 85
Diffie-Hellman key exchange
  IKE Phase 1
    planning, 499
    tunnel negotiations, 470
  PKI, 444
  running, 471
  VPNs, 438
digital certificates. See certificates
digital signatures, 438
    creating, 445
    DSA, 444
    RSA, 460
    VPN functions, 435-436
directed broadcasts, disabling, 87
disabling
    BOOTP service, 84
    CDP, 84
    Finger service, 84
    gratuitous ARPs, 85
    ICMP redirects, 86
    identification services, 84
    IP directed broadcasts, disabling, 87
    IP mask reply messages, 87
    IP source routing, 85
    IP unreachables, 87
    MOP, 87
    proxy ARPs, 86
    signatures, 401
    SNMP, 86
    TCP small servers service, 84
    UDP small servers service, 84
disaster recovery planning, 33
Distributed Denial-of-Service attacks (DDoS), 17
DMZ (demilitarized zone), 334
DNS (Domain Name Service)
    AnyConnect clients, configuring, 548
    ZBFs, configuring, 305
domain name configurations
    (AnyConnect client), 548
DoS (Denial-of-Service) attacks, 17
    IPv6, 211-212
    preventing, 59
    TCP SYN-flood attacks, 240
downloading practice exams, 560
DSA (Digital Signature Algorithm), 444
dual stacks (IPv6 risks), 214
dynamic ARP, 228
Dynamic ARP inspection (DAI), 59
Dynamic Host Configuration Protocol.
    See DHCP
dynamic NAT, 281
dynamic PAT, 281, 358

E

eavesdropping, 212
ECC (Elliptic Curve Cryptography), 444
editing. See customizing
ElGamal, 444
e-mail policies, 30
enabling
    AAA, 87
    CEF, 85
    firewalls, 87
    logging, 85
    password encryption services, 85
    RPF, 87
    signatures, 401, 404-405
    split tunneling, 554
    SSH, 87
    TCP keepalives, 85
    Telnet settings, 86
encryption
    asymmetric algorithms, 438
        examples, 444
        key length, 444
        overview, 433
communications
    best practices, 95
    HTTPS, implementing, 125
    SSH, implementing, 122-124
IKE Phase 1
  planning, 499
  tunnel negotiations, 470
IKE Phase 2, planning, 501
IPS/IDS, 381
management protocols, 103-104
SNMPv3, 130
symmetric algorithms, 432-433, 438
traffic
  after IPsec, 473
  before IPsec, 472-473
  identifying, 475
  IKE Phase 2, planning, 501
  IPsec, 472, 480-481
end zones (borderless), 41
enforcement
  guidelines, 31
  packet-filtering ACLs, 241-242
  policies. See policies
  procedures, 31
  standards, 31
err-disabled ports, restoring, 191-192
evasion methods (IPS/IDS), 381
  encryption/tunneling, 381
  protocol level misinterpretation, 381
  resource exhaustion, 381
  timing attacks, 381
  traffic
    fragmentation, 381
    substitution/insertion, 381
evidence, collecting, 32
exam updates, 573-574
  companion website, 573
  print version versus online version, 574
extended ACLs
  defined, 242
  identifying, 242
object groups
  applying, 253-254
  creating, 251-253
rules, applying, 251
standard ACLs, compared, 243
verifying, 254
external risk assessment, 27

F
false negatives (IPS/IDS), 377
false positives (IPS/IDS), 377
FE80 (link local addresses), 206
features
ASA firewalls, 230
  AAA, 230, 333
  ACLs (packet-filtering), 230
  application inspection/awareness, 331-332
  availability, 333
  botnets, filtering, 333
  DHCP, 332
  IPS (Intrusion Prevention System), 230
  Layer 2/Layer 3 implementations, 332
  management protocols, 230
  MPF, 230
  NAT support, 332
  object groups, 333
  packet filtering, 331
  routing, 230, 332
  stateful filtering, 230, 331
  URL filtering, 230
  VPNs, 230, 333
IOS router security, 228
routers, 227-229
  AAA, 229
  ACLs (packet-filtering), 229
CBAC, 229
control plane protection/policing, 229
IPS, 229
management protocols, 229
reflexive access lists, 229
routing protocol authentication, 229
VPNs, 229
Zone-Based Firewalls, 229
SSL, 534
switches, 227
BPDU guards, 228
DHCP snooping, 228
dynamic ARP inspections, 228
IP source guards, 228
modules, 228
port security, 228
root guards, 228
storm control, 228
ZBFs, 294-295
FF02::1 (multicast address), 206
files
IOS, protecting, 106
log, viewing, 258
primary bootset, storing, 132
signatures
configuration files, locating, 397
locations, defining, 396
obtaining, 393-394
public key, adding, 397
system, protecting, 96
filtering
ASA packet, 331, 337-338
implementing, 338
inbound traffic, 337-338
outbound traffic, 338
bogus addresses, 214
botnets, 333
ICMP unused traffic, 215
IPv4 packet
ACLs, creating, 246
applying ACLs to interfaces, 249
CLI implementation, 248
lines, adding, 246
object groups, 251-254
ordering, 247
policies, 244
rules, applying, 251
summary page (CCP), 245
verifying, 254
IPv6 packet, 259-262
creating and applying, 261-262
ICMP, 262
objectives, 260
topology, 260
non-local multicast addresses, 215
packet-filtering ACLs, 239
ASA firewalls, 230
creating policies, 241
enforcing policies, 241-242
firewalls, 285
routers, 229
SDEE log file screen, 414
signatures, based on signature IDs, 402
stateful, 276-277
ASA, 331
ASA firewalls, 230
static packets, 274-275
traffic, 212
URLs, 230
final review/study plan, 562
Finger service, disabling, 84
firewalls
access rules, 284
application inspection, 276
application layer gateways, 275
ASA, 42
AAA support, 333
access rules, 359-362
ACLs, 239
application inspection/awareness, 331-332
ASDM, 345-347
availability, 333
botnets, filtering, 333
client IP addresses, 355
configuring, 340-345
connectivity, testing, 345
console ports, connecting, 337
default traffic flow, 335-336
DHCP, 332
initial boot, 340-345
interfaces, configuring, 347-355
Layer 2/Layer 3 implementations, 332
managing, 336-337
models, 330-331
MPF, 338-339
NAT, 332, 357-359
object groups, 333
packet filtering, 331, 337-338
Packet Tracer, 362-367
PAT, 357-359
policies, applying, 339-340
routing, 332, 356-357
security features, 230
security levels, 333-334
self-signed certificates, 454
setup script, running, 343-345

stateful filtering, 331
VPN support, 333
capacities, 273
defense in depth, 272-273
designing, 283-284
DMZ, 334
enabling, 87
implementing, 274
IOS support, 58
limitations, 272
logs viewing, 259
NAT, 278-281
deployment options, 281
inside/outside/local/global terminology, 279
PAT, 279-281
source IP addresses, 278-279
objectives, 270-271
packet-filtering ACLs, 285
protecting against
exposure of sensitive systems to untrusted individuals, 271
malicious data, 271
protocol flaw exploitation, 271
unauthorized users, 271
rules
access, 284
guidelines, 285-286
implementation consistency, 286-287
stateful packet filtering, 276-277
static packet filtering, 274-275
technologies, 270, 283
transparent, 276-278
ZBFs, 229
administrator created zones, 295
class maps, 296
components, configuring, 298-300
configuring, 300-313
monitoring, 314-315
NAT, configuring, 319-322
NAT, verifying, 322-323
overview, 294
policy maps, 296-297
self zones, 297-298
service policies, 297
traffic interaction between zones, 297-298
verifying with CCP, 314-315
verifying with command line, 315-319
zone pairs, 295
formatting IPv6 addresses, 202-204
fragmenting traffic, 381
frameworks
MPF, 230, 338-339
NFP (network foundation protection), 52-53
control, 52
data, 53
interdependence, 53
management, 52
full-tunnel SSL VPN. See AnyConnect SSL VPNs

G

gateways (application layer)
firewalls, 275
general security posture assessment, 27
GET messages, 129
global correlation, 382, 386
global NAT, 279
governmental asset classifications, 11
gratuitous ARPs, disabling, 85
groups
AnyConnect SSL VPNs, 552-553
device
creating, 156
network devices, adding, 157-158
object
applying, 253-254
creating, 251-253
overview, 244
signatures, 384
SSL VPN users, assigning, 538
user, creating, 158
guards
BPDU
implementing, 190-191
switches, 228
IP source, 228
root, 192, 228
guidelines, 16
auditing, 16
defense in depth, 16
policies, 29
rule of least privilege, 16
separation of duties, 16
H

Hashed Message Authentication Code (HMAC), 434
hashes, 434
data integrity, verifying, 428-430, 434
HMAC (Hashed Message Authentication Code), 434
IKE Phase 1
planning, 499
tunnel negotiations, 470
IKE Phase 2, planning, 501
overview, 434
types, 434
headers (IPv6)
  IPv6 versus IPv4, 203
  risks, 214
  routing header 0s, dropping, 215
Help icon (CCP toolbar), 68
hexadecimal/binary/decimal conversions, 204
hierarchical PKI topology, 453
HIPAA (Health Insurance Portability and Accountability Act), 28
HMAC (Hashed Message Authentication Code), 434
Home button (CCP toolbar), 68
HTTP (Hypertext Transfer Protocol), 87
HTTPS (Hypertext Transfer Protocol Secure), 125

ICMP (Internet Control Message Protocol), 86
IPv6
  packet filtering, 262
  risks, 214
mask reply messages, disabling, 87
redirects, disabling, 86
unreachables, disabling, 87
unused traffic, filtering, 215
identity certificates, 448
installing with SCEP, 457-459
  CA server details, 457
  command line, 458-459
  details, viewing, 459
  enrollment modes, 458
  key pairs, creating, 457
  success message, 459
manually installing, 456
requesting, 450
Identity Service Engine. See ISE
IDS (Intrusion Detection System), 374
  advantages/disadvantages, 379
  alerts, delivering, 385
  best practices, 386
  countermeasure actions, 379-380
    deny attacker inline, 380
    deny connection inline, 380
    deny packet inline, 380
    log attacker packets, 380
    log pair packets, 380
    log victim packets, 380
    produce alert, 380
    produce verbose alert, 380
    request block connection, 380
    request block host, 380
    request SNMP trap, 380
evasion methods, 381
  encryption/tunneling, 381
  protocol level misinterpretation, 381
  resource exhaustion, 381
  timing attacks, 381
  traffic fragmentation, 381
  traffic substitution/insertion, 381
false positives/negatives, 377
information accuracy, 376
intelligence
  collecting, 385-386
  global correlation, 386
IPS, compared, 374-376
malicious traffic, identifying, 377
  anomaly-based, 378
  method advantages/disadvantages, 379
  policies, 378
  reputation-based, 378-379
  signatures, 377-378
implementing AAA
   CCP, 116-118
   command line, 113-115
   debug command, 115
actions based on risk ratings, 381
ASA packet filtering, 338
BPDU guards, 190-191
dynamic PAT, 358
firewalls, 274
   application inspection, 276
   application layer gateways, 275
   best practices, 283-284
   interfaces, 352-355
   NAT, 278-281
   rules, 286-287
   stateful packet filtering, 276-277
   static packet filtering, 274-275
   technologies, 283
   transparent, 276-278
HTTPS, 125
IPv4 packet filtering
   ACLs, creating, 246
   applying ACLs to interfaces, 249
   CLI implementation, 248
   lines, adding, 246
   object groups, 251-254
   ordering, 247
   policies, 244
   rules, applying, 251
   summary page (CCP), 245
   verifying, 254
IPv6 packet filtering, 259-262
   creating and applying, 261-262
   ICMP, 262
   objectives, 260
topology, 260
implementing logging, 125-127
  CCP configuration, 126
  settings, editing, 126-127
  syslog output, viewing, 127
  syslog support, configuring, 125-126

NAT, 357
NFP (network foundation protection)
  auto secure utility, 53
  plane protection, 53-54

NTP, 502-504
parser views, 120-122
port security, 192-194
RBAC, 118-120
  parser views, 120-122
  privilege levels, customizing, 118-120

security policies, 231
SSH, 122-124
SSL VPNs, 533
strong passwords, 106-108
use authentication, 108-113

in-band management, 96
inbound traffic (ASA firewalls), 337-338
incident response policies, 32, 226
infrastructure, 52. See also NFP
inside NAT, 279
installing
  AnyConnect client, 550
  CD (book), 560
  IOS-based IPS from command line, 407-412
  IOS-based IPS with CCP, 394-400
    configuration screen navigation, 394
    deployment bit on CPU resources, 398
    interfaces, choosing, 396

IPS policy welcome page, 395
  public key, adding, 397
  router subscriptions, opening, 395
  SDEE, enabling, 395
  signature file locations, defining, 396-397
  signatures, compiling, 399-400
  summary page, 398
  traffic inspection direction, 396
  public keys, 397

Integrated Services Routers (ISR), 42

integrity
  data. See data integrity defined, 8
  SNMPv3, 130
interdependence (NFP planes), 53

interfaces
  ACLs, applying, 249
  CCP
    content pane, 69
    left navigation pane, 67
    menu bar, 66
    status bar, 69
    toolbar, 67-68
clientless SSL VPNs, configuring, 537
default traffic flow, 335-336
firewalls
  configuring, 347-355
  editing, 351
  final configuration, 352
  implementing, 352-355
  maximum allowed, 350
  summary page, 350
  VLAN number associations, 349-350
IKE Phase 2, planning, 501
IPS policies, applying, 396
IP addresses

AnyConnect VPN clients, assigning, 548
hosts, assigning, 203
IKE Phase 2, planning, 501
IPv6 versus IPv4, 203
management sessions, controlling, 56
source
  interfaces, testing, 515-516
  NAT, 278-279
spoofing attacks, preventing, 240
IP protocol
  BOOTP service, disabling, 84
  CEF, enabling, 85
directed broadcasts, disabling, 87
gratuitous ARPs, disabling, 85
Identification services, disabling, 84
IPv6. See IPv6
source
  guards, 59, 228
  routing, disabling, 85
IP Security. See IPsec
IPS (Intrusion Prevention System), 43, 58
advantages/disadvantages, 379
alerts, delivering, 385
ASA firewalls, 230
best practices, 386
countermeasure actions, 379-380
  deny attacker inline, 380
  deny connection inline, 380
  deny packet inline, 380
  log attacker packets, 380
  log pair packets, 380
  log victim packets, 380
  produce alert, 380
  produce verbose alert, 380
  request block connection, 380
  request block host, 380
  request SNMP trap, 380
data plane protection, 59
evasion methods, 381
  encryption/tunneling, 381
  protocol level misinterpretation, 381
  resource exhaustion, 381
timing attacks, 381
traffic fragmentation, 381
traffic substitution/insertion, 381
false positives/negatives, 377
IDS, compared, 374-376
information accuracy, 376
intelligence, 385-386
IOS-based
  alarm summarization, 392
  alerts, 412-416
  anti-evasive techniques, 392
  benefits, 392
  detection methods supported, 392
  features, 392
  installing from command line, 407-412
  installing with CCP, 394-400
  regular expression string pattern matching, 392
  requirements, 393
  response actions, 392
  risk ratings, 392
  signature files, obtaining, 393-394
  threshold configuration, 392
  tuning, 412
IPv6, 381
malicious traffic, identifying, 377
  anomaly-based, 378
  method advantages/disadvantages, 379
  policies, 378
  reputation-based, 378-379
  signatures, 377-378
risk ratings, 379-382
  actions, implementing, 381
  factors, 379-382
routers, 229
security, implementing, 231
sensors
defined, 374
  platforms, 375-376
signatures, 384-385
  ASR (attack severity rating), 384-385
groups, 384
micro-engines, 384
SFR (signature fidelity rating), 385
true positives/negatives, 377
IPS Policies wizard, 395
IPSec
configuring, 475-484
  command line, 482-484
  IKE Phase 1 policy, 477-478
  local Ethernet information, entering, 477
mirrored VPN for remote peers, 485-486
remote peer information, entering, 477
Step by Step wizard, 476
summary, 481
traffic encrypting, 472
  identifying for encryption, 475
  before IPsec, 472-473
  after IPsec, 473
verifying, 486-490
VPNs, 427, 436-437
IPv4
IPv6, comparison, 202-203
packet filtering
  ACLs, creating, 246
  applying ACLs to interfaces, 249
  CLI implementation, 248
  lines, adding, 246
  object groups, 251-254
  ordering, 247
  policies, 244
  rules, applying, 251
  summary page (CCP), 245
  verifying, 254
IPv6
addresses
  128-bit, 203
  all-nodes multicast, 206
all-routers multicast, 206
decimal/binary/hexadecimal conversions, 204
formatting, 202-204
hexadecimal hard way example, 204-205
link local, 205-206
loopback, 206
multicast, 207
remote device communication, 205
solicited-node multicast, 207
unicast/anycast, 206-207
zero shortcuts, 205
application layer protocols support, 203
benefits, 202
bogus addresses, filtering, 214
headers, 203
ICMP unused traffic, filtering, 215
IP addresses, 203
IPS, 381
IPsec support, 203
IPv4, compared, 202-203
Layer 2 support, 203
Layer 4 protocols support, 203
migration, 210
NAT, 203
NDP (Neighbor Discovery Protocol), 203
network masks, 203
non-local multicast addresses, filtering, 215
packet filtering, implementing, 259-262
creating and applying, 261-262
ICMP, 262
objectives, 260
topology, 260
risks, 213-214
autoconfiguration, 214
bugs, 214
DHCP, 213
dual stacks, 214
hop-by-hop extension headers, 214
ICMP, 214
NDP, 213
packet amplification attacks, 214
tunneling, 214
rogue devices, 215
routing
configuring, 208-210
header 0s, dropping, 215
router output example, 207-208
security
advantages, 213
best practices, 210-211
policies, 211
threats
application layer, 212
DoS attacks, 212
man-in-the-middle attacks, 212
router attacks, 213
sniffing/eavesdropping, 212
spoofed packets, 212
unauthorized access, 212
tunneling, 215
IronPort Email Security/Web Security Appliances, 43
ISE (Identity Service Engine)
ACS, compared, 141
user authentication, 14
ISR (Integrated Services Routers), 42
issuers (certificates), 447, 449
key pairs
creating, 457
overview, 460
keys, 431
asymmetric encryption algorithms, 432-433, 438
block ciphers, 432
Diffie-Hellman key exchange, 438
keyspace, 436
lengths, 433
managing, 436
OTP (one-time pad), 431
PKI. See PKI
public
algorithms, 433
certificates, 448-449
exchanging, 445
installing, 397
peers, obtaining, 448
public key cryptography.
See asymmetric algorithms
stream ciphers, 432
symmetric encryption algorithms, 432-433, 438

trunking
automatic switch negotiation, 182
native VLANs, 181
negotiations, not allowing, 190
topology, 178
traffic, tagging, 180-181
VLANs
access ports, assigning, 178-179
frames, following, 181
inter-VLAN routing, 182
negotiations, not allowing, 190
overview, 178
physical interfaces disadvantage, 182
PVST+, 187
router on a stick, 182
STP. See STP
subinterfaces, creating, 182-183
switch ports, locking down, 189-190
topology, 178
Layer 3, 332
Layer 4 protocols
  50, 500
  51, 500
IPv6 versus IPv4, 203
left navigation pane (CCP), 67
lengths
  keys
    asymmetric, 444
    symmetric, 433
passwords, setting, 85
liabilities, 33
licensing
  ACS, 156
  CCP, 65
lifecycles
  loops, 184
  security, 25
lifetime
  IKE Phase 1
    planning, 499
    tunnel negotiations, 470
  IKE Phase 2, planning, 501
lines (ACLs)
  adding, 246
  numbers, 243
link local addresses, 205-206
list-name command, 102
local NAT, 279
local users (ACS routers), adding, 153-154
logging
  ACLs
    firewall log details, 259
    logs, viewing, 258
    summary syslog messages, 257
    syslog destinations, 258
  attacker packets, 380
  best practices, 96
  configuring, 126
  enabling, 85
  implementing, 125-127
  output destinations, sending, 104-105
  pair packets, 380
  SDEE log file screen
    filtering, 414
    searching, 414
    viewing, 413-414
  settings, editing
    CCP, 126
    command line, 127
  syslog, 105
    destinations, 258
    locking down, 56
    output, viewing, 127
    support, configuring, 125-126
  victim packets, 380
  viewing, 104
logging in (clientless SSL VPNs), 541
logical boundaries, 40-41
  data centers, 41
  end zones, 41
  Internet, 41
  policy management points, 41
logical controls, 12
login screen (ACS), 156
loopback addresses, 206
loops (Layer 2)
  lifecycle, 184
  solution, 184-187

M
MAC addresses
  flooding, 59
  port security, 192-194
Maintenance Operations Protocol, 87
malicious data, protecting against, 271
malicious traffic
general vulnerabilities, 241
identifying, 377
  anomaly-based, 378
  method advantages/disadvantages, 379
  policy-based, 378
  reputation-based, 378-379
  signature-based, 377-378
IP address spoofing, 240
reconnaissance attacks, 240-241
risks, reducing. See IPS/IDS
sensor responses, 379-380
  deny attacker inline, 380
  deny connection inline, 380
  deny packet inline, 380
  log attacker packets, 380
  log pair packets, 380
  log victim packets, 380
  produce alert, 380
  produce verbose alert, 380
  request block connection, 380
  request block host, 380
stopping, 239-240
TCP SYN-flood attacks, 240
man-in-the-middle attacks, 14-16, 212
Manage Community dialog box, 71
Manage Community icon (CCP toolbar), 68
Management Information Base (MIB), 128
management plane
AAA, 55
  accounting/auditing, 98
  authentication, 98
  authorization, 98
  best practices, 97-98
  CCP implementation, 116-118
  command line implementation, 113-115
  method lists, creating, 101-102
  router access authentication, 100
  usernames/passwords/access rules storage, 98-99
  VPN users, 99-100
  defined, 52, 94
encrypted communications
  best practices, 95
  HTTPS, implementing, 125
  management protocols, 103-104
  SSH, implementing, 122-124
IOS files, protecting, 106
IP addresses, controlling, 56
logging, 104-105
  best practices, 96
  configuring, 126
  implementing, 125-127
  output destinations, sending, 104-105
  settings, editing, 126-127
  syslog, 105
  syslog output, viewing, 127
  syslog support, configuring, 125-126
  viewing, 104
NTP
  authentication, 132
  CCP configuration, 131
  configuring, 131-132
  synchronization, verifying, 132
overview, 55
passwords
  policies, 55
  recommendations, 97
  strong, 95, 106-108
primary bootst storage, 132
RBAC, 55, 101-103
best practices, 95
implementing, 118-122
parser views, 103, 120-122
privilege levels, customizing, 103, 118-120
remote connections, 94
security measures, 54
SNMP, 128-131
agent, 128
CCP configuration, 130-131
command line configuration, 131
defined, 128
manager, 128
message types, 129
MIB, 128
security levels, 129
security model, 129
sending/receiving information vulnerability, 129
v1/v2 security weaknesses, 129
v3 enhancements, 130
v3 security levels, 129
syslog lockdown, 56
system files, 96
time accuracy, 56, 96, 105-106
user authentication
best practices, 95
implementing, 108-113
management protocols
ASA firewalls, 230
encrypting, 103-104
router security, 229
management traffic, 94
managing
ASAs, 336-337
bandwidth, 59
in-band management, 96
keys, 436
risks
attackers, becoming, 32-33
disaster recovery/business continuity planning, 33
evidence, collecting, 32
guidelines, 31
incident responses, 32
liabilities, 33
new assets, 27-28
policies, 31
procedures, 31
standards, 31
testing security, 30
transferring to someone else, 13
signatures
ASR (attack severity rating), 384-385
groups, 384
micro-engines, 384
SFR (signature fidelity rating), 385
masks
network, 203
reply messages, disabling, 87
wildcard, 244
maximum tolerable downtime (MTD), 33
memory (CAM overflow attacks), 59
memory tables, 561
menu bar (CCP), 66
merging options (CCP templates), 77-78
messages (SNMP), 129
method command, 102
method lists (AAA)
ACS authentication
routers, configuring, 144, 149-150
testing, 166-170
ACS authorization
   routers, configuring, 144, 150-151
testing, 166-170
applying, 152
creating, 101-102, 144
methods of attacks, 14-15
   back doors, 15
   botnets, 17
c covert channels, 17
DoS/DDoS, 17
passwords, 17
privilege escalation, 15
reconnaissance, 15
social engineering, 15
trust exploitation, 17
MIB (Management Information Base), 128
micro-engines, 384
   IOS-based IPS, 399-400
migrating IPv6, 210
models (ASA family), 330-331
Modular Policy Framework (MPF), 230, 338-339
modules (switches), 228
Monitor button (CCP toolbar), 68
monitoring
   ACLs, 255-257
   SSL VPN sessions, 543-544
threats
   ASA firewalls, 42
centralized, 226
   IPS (Intrusion Prevention System), 43
   IronPort Email Security/Web Security Appliances, 43
   ISR (Integrated Services Routers), 42
   prevention tools, 42-43
   ScanSafe, 43
ZBFs, 314-315
MOP (Maintenance Operations Protocol), 87
MPF (Modular Policy Framework), 230, 338-339
MPLS (Multiprotocol Label Switching), 427
MTD (maximum tolerable downtime), 33
multicast addresses, 207
   all-nodes, 206
   all-routers, 206
   non-local, filtering, 215
   solicited-node, 207
multistring micro-engine, 384

N

NAC (Network Admission Control), 14
names (interfaces), 334
NAT (Network Address Translation), 203
   ACLs, 239
   AnyConnect VPN exemptions, 549
   ASAs, 357-359
      implementing, 357
      verifying, 358
   ASA support, 332
   configuring
      CCP, 319-321
      command line, 322
dynamic, 281
firewalls, 278-281
   deployment options, 281
   inside/outside/local/global terminology, 279
   PAT, 279-281
   source IP addresses, 278-279
IPv6 versus IPv4, 203
policy-based, 281
static, 283
terminology, 279
verifying, 322-323
wizard, 319-321
National Vulnerability Database, 12
native VLANs, 181
NDP (Neighbor Discovery Protocol), 203, 213
Network Address Translation. See NAT
Network Admission Control (NAC), 14
network foundation protection. See NFP
network masks, 203
network policies, 30
Network Time Protocol. See NTP
NFP (network foundation protection), 49
control plane
   CoPP, 56
   CPPr, 56
defined, 52
   nontransit traffic, 56
   protection/policing, 229
   routing protocol authentication, 56
   security measures, 54
data plane
   ACLs, 58
   bandwidth management, 59
   CAM overflow attacks, 59
   DAI, 59
defined, 53
   DHCP snooping, 59
   DoS attacks, reducing, 59
   IOS firewall support, 58
   IOS IPS, 58
   IP source guard, 59
   IPS (Intrusion Prevention System), 59
   MAC address flooding, 59
   security measures, 54
   spoofing attacks, preventing, 59
   TCP intercept, 58
   transit traffic, 56
   unicast reverse path forwarding, 58
   unwanted traffic, blocking, 59
framework
   interdependence, 53
   planes, 52-54
implementing
   auto secure utility, 53
   plane protection, 53-54
infrastructure importance, 52
management plane
   AAA implementation, 113-118
defined, 52, 94
   encrypted/authenticated SNMP, 56
   encrypted communications, 95
   encrypted management protocols, 103-104
   HTTPS, implementing, 125
   IOS files, protecting, 106
   IP addresses, controlling, 56
   logging, 96, 104-105, 125-127
   NTP, configuring, 131-132
   overview, 55
   password policies, 55
   password recommendations, 97
   primary bootset storage, 133
   RBAC, 55, 95, 101-103, 118-122
   remote connections, 94
   security measures, 54
   SNMP, 128-131
   SSH, implementing, 122-124
   strong passwords, 95, 106-108
syslog lockdown, 56
system files, 96
time accuracy, 56, 96, 105-106
user authentication, 95, 108-113
noAuthNoPriv security level (SNMP), 129
non-local multicast addresses, filtering, 215
nontransit traffic protection, 56
CoPP, 56
CPPr, 56
routing protocol authentication, 56
NTP (Network Time Protocol), 96
authentication, 132
best practices, 105-106
configuring, 131-132
site-to-site VPNs, implementing, 502-504
synchronization, verifying, 132
NVD (National Vulnerability Database), 12

O

object groups
applying, 253-254
ASA, 333
creating, 251-253
overview, 244
objectives, 8
availability, 9
confidentiality, 8
configuring routers for ACS servers, 142-144
integrity, 8
One-Step Lockdown (CCP Security Audit), 84
one-time pad (OTP), 431
ordering ACLs, 247
OSCP (Online Certificate Status Protocol), 452

OTP (one-time pad), 431
outbound traffic
ACLs, 242
ASAs, 338
output (syslog), 127
outside NAT, 279
override options (CCP templates), 77-78
owners (asset classification), 11

P

Packet Tracer, 362-367
command line, 364-366
input, configuring, 332-362
launching, 362
results, 363-364
Telnet denial, verifying, 366-367
packets
amplification attacks, 214
ASA filtering, 331, 337-338
implementing, 338
inbound traffic, 337-338
outbound traffic, 338
encrypting (IPsec), 472
filtering (ACLs), 239
ASA firewalls, 230
creating policies, 241
enforcing policies, 241-242
firewalls, 285
IPv4. See IPv4, packet filtering
routers, 229
Packet Tracer, 362-367
command line, 364-366
input, configuring, 332-362
launching, 362
results, 363-364
Telnet denial, verifying, 366-367
spoofed, mitigating, 212
stateful filtering
  ASA firewalls, 230
  firewalls, 276-277
static packet filtering, 274-275

parser views
creating, 103, 121-122
implementing, 120-122
user accounts, assigning, 122

passwords
ASDM, 345
attacks, 17
authentication failure rates, 85
enable secret password, setting, 86
encryption services, enabling, 85
management plane, securing, 55
minimum lengths, setting, 85
recommendations, 97
storing, 98-99
strong
  best practices, 95
  implementing, 106-108

PAT (Port Address Translation), 239
ACLs, 239
ASAs, 332, 357-359
dynamic, 281
firewalls, 279-281
policy-based, 281
rules verification, 358

Pearson IT Certification Practice
Test engine, 559
activating/downloading, 560
CD software, installing, 560
modes, 563
navigating, 563

peer authentication
IKE Phase 1, 471
IPsec, 468-469

Per-VLAN Spanning Tree Plus (PVST+), 187
PFS (Perfect Forward Secrecy), 501
pharming, 15
phases (security lifecycles), 25
phishing, 15
physical controls, countermeasures, 12
physical security (IPv6), 210

ping command
IPsec traffic triggers, 512
routers, 499
router-to-ACS connections, 164
signatures, 406
source interfaces with associated IP
  addresses, 515-516

PKCS (Public Key Cryptography Standards), 450, 460
PKI (Public Key Infrastructure), 441
asymmetric algorithms
  examples, 444
  key length, 444
  overview, 433
certificate authorities, 446, 460
  authenticating, 450
  certificate information, 446
  commercial, 446
  enrolling, 450
certificates, 460
  ASA self-signed, 454
  functions, 452
  identity, 448
  issuers, 449
  peers public keys, obtaining, 448
  public keys, 449
  revocation list location, 449
  revoked, 451-452
  root, 446-448
SCEP root/identity certificates
installations, 457-459
serial numbers, 449
signatures, 449
subjects, 449
thumbprint, 449
validity dates, 449
viewing in ASDM, 455
X.500/X.509v3, 449
X.500/X.509v3 certificates, 460
components, 461
key pairs, 444
PKCS (Public Key Cryptography
Standards), 450, 460
public-private key pairs, 460
RSA
digital signatures, creating,
445, 460
public keys, exchanging, 445
public-private key pairs, 445
SCEP (Simple Certificate Enrollment
Protocol), 451
subordinate CA, 460
topologies, 453
cross-certifying CAs, 453
hierarchical with subordinate
CAs, 453
single root CAs, 453

planes (NFP), 52-53
control, 54
CoPP, 56
CPPr, 56
defined, 52
nontransit traffic, 56
protection/policing, 229
routing protocol authentication, 56
security measures, 54
data
ACLs, 58
bandwidth management, 59
CAM overflow attacks, 59
DAI, 59
defined, 53
DHCP snooping, 59
DoS attacks, reducing, 59
IOS firewall support, 58
IOS IPS, 58
IP source guard, 59
IPS (Intrusion Prevention
System), 59
MAC address flooding, 59
security measures, 54
spoofing attacks, preventing, 59
TCP intercept, 58
transit traffic, 56
unicast reverse path forwarding, 58
unwanted traffic, blocking, 59
interdependence, 53
management
AAA implementation, 113-118
defined, 52, 94
encrypted/authenticated SNMP, 56
encrypted communications, 95
encrypted management protocols,
103-104
HTTPS, implementing, 125
IOS files, protecting, 106
IP addresses, controlling, 56
logging, 96, 104-105, 125-127
NTP, configuring, 131-132
overview, 55
password policies, 55
password recommendations, 97
primary bootset storage, 132
RBAC, 55, 95, 118-122
remote connections, 94
security measures, 54
SNMP, 128-131
SSH, implementing, 122-124
strong passwords, 95, 106-108
syslog lockdown, 56
system files, 96
time accuracy, 56, 96, 105-106
user authentication, 95, 108-113

platforms
ACS supported, 141
sensors, 375-376

policies
ASA
applying, 339-340
MPF, 338-339
authorization, 161-163
crypto, configuring, 508-510
IKE Phase 1
configuring, 506-507
creating, 477-478
planning, 499-500
IKE Phase 2, 501-502
configuring, 507-510
encryption, 501
hashes, 501
interfaces, selecting, 501
lifetimes, 501
peer IP addresses, 501
PFS (Perfect Forward Secrecy), 501
traffic encryption, 501
incident responses, 32, 226
IPv6, 211
management points, 41
packet-filtering ACLs
creating, 241
enforcing, 241-242

password, 55
security
application, 30
content, 28
creators, 28
defined, 31
e-mail, 30
formal procedures, 226
functions, 28
guideline, 29
implementing, 231
network, 30
overview, 28
remote-access, 30
telephony, 30
types, 29-30

service
defined, 297
traffic interaction between zones, 297-298
threat mitigation, 226

policy-based
IPS/IDS, 378
NAT, 281
PAT, 281

policy maps
actions, 297
ASAs, 339
defined, 296

polyalphabetic ciphers, 431
Port Address Translation. See PAT
ports
access
assigning to VLANs, 178-179
negotiations, not allowing, 190
err-disabled, restoring, 191-192
root guards, 192
security, implementing, 192-194, 228
STP caution towards new, 187
switch
  BPDU guards, 190-191
  locking down, 189-190
trunk
  automatic switch negotiation, 182
  traffic tags, creating, 180-181
potential attackers, 13-14
  motivations/interests, understanding, 14
  not becoming, 32-33
  types, 13
practice exams, 559
  activating/downloading, 560
  CD software, installing, 560
  Premium Edition practice exams, 561
Premium Edition practice exams, 561
prevention strategies (borderless networks), 42-43
  ASA firewalls, 42
  IPS (Intrusion Prevention System), 43
  IronPort Email Security/Web Security Appliances, 43
  ISR (Integrated Services Routers), 42
  ScanSafe, 43
previewing CCP commands, 83
primary bootset, storing, 132
private sector asset classifications, 11
privileges
  escalation, 15
  levels, customizing, 103, 118-120
procedures, 31
profiles
  AnyConnect SSL VPN connection, 545
  authorization, 162
  user (CCP), 78-80
    applying, 80
    creating, 79
  restrictions, 78
  saving, 80
  verifying, 80
protection
  administrator access/protocols, 55-56
    AAA services, 55
    encrypted/authenticated SNMP, 56
    IP addresses, 56
    password policies, 55
    RBAC, 55
    syslog lockdown, 56
    time accuracy, 56
  IOS files, 106
  network foundation. See NFP
  nontransit traffic, 56
  system files, 96
  traffic, 480-481
  transit traffic, 56
  ACLs, 58
    bandwidth management, 59
    CAM overflow attacks, 59
    DAI, 59
    DHCP snooping, 59
    DoS attacks, preventing, 59
    IOS firewall support, 58
    IOS IPS, 58
    IP source guard, 59
    IPS (Intrusion Prevention System), 59
    MAC address flooding, 59
    spoofing attacks, preventing, 59
    TCP intercept, 58
    unicast reverse path forwarding, 58
    unwanted traffic, blocking, 59
protocols
ACS server/router communication, 141-143
choosing, 142-143
RADIUS, 142
TACACS+141
administrator, protecting, 55-56
AAA services, 55
encrypted/authenticated SNMP, 56
IP addresses, controlling, 56
password policies, 55
RBAC, 55
syslog lockdown, 56
time accuracy, 56
AnyConnect SSL VPNs, choosing, 546
application layer, 203
ARPs
dynamic, 228
gratuitous, disabling, 85
proxy, disabling, 86
CDP, disabling, 84
DHCP
ASA, 332, 355
IPv6 risks, 213
IPv6 versus IPv4, 203
snooping, 59, 228
flaws, exploiting, 271
HTTPS, implementing, 125
ICMP
IPv6 packet filtering, 262
IPv6 risks, 214
mask reply messages, disabling, 87
redirects, disabling, 86
unreachables, disabling, 87
unused traffic, filtering, 215
IKE Phase 1, choosing, 475
IKE Phase 2, choosing, 475
IP
BOOTP service, disabling, 84
CEF, enabling, 85
directed broadcasts, disabling, 87
gratuitous ARPs, 85
identification services, disabling, 84
IPv6. See IPv6
source guards, 59, 228
source routing, disabling, 85
IPsec. See IPsec
IPv6
128-bit addresses, 203
all-nodes multicast addresses, 206
all-routers multicast addresses, 206
application layer, 203, 212
benefits, 202
bogus addresses, filtering, 214
decimal/binary/hexadecimal
conversions, 204
DoS attacks, reducing, 212
formatting addresses, 202-204
headers, 203
hexadecimal hard way example,
204-205
ICMP unused traffic,
filtering, 215
IP addresses, 203
IPS, 381
IPsec support, 203
IPv4, compared, 202-203
Layer 2 support, 203
Layer 4 protocols support, 203
link local addresses, 205-206
loopback addresses, 206
man-in-the-middle attacks, 212
migration, 210
multicast addresses, 207
NAT, 203
NDP (Neighbor Discovery Protocol), 203
network masks, 203
non-local multicast addresses, filtering, 215
packet filtering, 259-262
remote device communication, 205
risks, 213-214
rogue devices, 215
router attacks, 213
router output example, 207-208
routing, configuring, 208-210
routing header 0s, dropping, 215
security advantages, 213
security best practices, 210-211
sniffing/eavesdropping, 212
solicited-node multicast addresses, 207
spoofed packets, 212
tunneling, 215
unauthorized access threats, 212
unicast/anycast addresses, 206-207
zero shortcuts, 205
Layer 4
IPv6 versus IPv4, 203
protocol 50, 500
protocol 51, 500
level misinterpretations, 381
management
ASA firewalls, 230
encrypting, 103-104
router security, 229
MOP, disabling, 87
NDP, 203, 213
NTP, 96
authentication, 132
best practices, 105-106
CCP configuration, 131
configuring, 131-132
site-to-site VPNs, implementing, 502-504
synchronization, verifying, 132
OSCP (Online Certificate Status Protocol), 452
RADIUS
overview, 142
TACACS+, compared, 142-143
routing
ACLs, 239
ASA firewalls, 230
authentication, 56, 229-230
control plane, 56
IPv6, 211
routers, 229
SCEP (Simple Certificate Enrollment Protocol), 451, 457-459
secured management, 43
SNMP
agent, 128
CCP configuration, 130-131
certificate line configuration, 131
defined, 128
disabling, 86
logs, receiving, 104
management plane, 56
manager, 128
message types, 129
MIB, 128
security levels, 129
security model, 129
sending/receiving information vulnerability, 129
v1/v2 security weaknesses, 129
v3 enhancements, 130
v3 security levels, 129
SSL. See SSL
STP, 183

loop lifecycle, 184
new ports, 187
PVST+, 187
Rapid Spanning Tree, 187-188
verification/annotations, 184-187
TACACS+
overview, 141
RADIUS, compared, 142-143
TCP
intercept, 58
keepalives, enabling, 85
SYN-flood attacks, 240
SYN-Wait times, setting, 85
TLS, 532-534
Provide feedback to Cisco icon (CCP toolbar), 68
proxy ARPs, disabling, 86
Public Key Infrastructure. See PKI
certificates, 448-449
cryptography. See asymmetric algorithms
exchanging, 445
installing, 397
Peers, obtaining, 448
PVST+ (Per-VLAN Spanning Tree Plus), 187

QoS (Quality of Service), 239
qualitative risk analysis, 26
quantitative risk analysis, 26

R

RADIUS (Remote Authentication Dial-In User Service)
overview, 142
TACACS+, compared, 142-143
Rapid Spanning Tree, configuring, 187-188
RBAC (role-based access control), 55, 101-103
best practices, 95
implementing, 118-122
management plane, 55
parser views
best practices, 103
creating, 121-122
implementing, 120-122
user accounts, assigning, 122
privilege levels, customizing, 103, 118-120
reconnaissance attacks, 15, 240-241
recovery point objective (RPO), 33
recovery time objective (RTO), 33
redirects (ICMP), disabling, 86
reflexive access lists, 229
Refresh icon (CCP toolbar), 68
regular expressions, string pattern matching, 392
regulatory compliance, as risks, 28
remote-access policies, 30
VPNs, 427
Remote Authentication Dial-In User Service. See RADIUS
reports
ACS, 165-166
Security Audit Report Card, 82
reputation-based IPS/IDS, 378-379
request block sensor responses
  connections, 380
  hosts, 380
request SNMP trap sensor response, 380
restoring err-disabled ports, 191-192
retiring signatures, 401
Reverse Path Forwarding (RPF), 87
revocation list location (certificates), 449
revoked certificates, 451-452
risk ratings. See RRs
risks
  analysis, 25-26
    cost-benefit analysis, 9-10
    current posture assessment, 26-27
    qualitative, 26
    quantitative, 26
defined, 10
end users, 224-225
firewall protection against
  exposure of sensitive systems to untrusted individuals, 271
  malicious data, 271
  protocol flaw exploitation, 271
  unauthorized users, 271
IPv6, 213-214
  autoconfiguration, 214
  bugs, 214
  DHCP, 213
  dual stacks, 214
  hop-by-hop extension headers, 214
  ICMP, 214
  NDP, 213
  packet amplification attacks, 214
  tunneling, 214
managing, 26-28
  assuming, 13
  attackers, becoming, 32-33
  disaster recovery/business continuity planning, 33
  evidence, collecting, 32
  guidelines, 31
  incident responses, 32
  liabilities, 33
  new assets, 27-28
  policies, 31
  procedures, 31
  standards, 31
  testing security, 30
  transferring to someone else, 13
regulatory compliance, 28
threat mitigation/containment strategies, designing, 224
Rivest, Shamir, Adleman.
  See RSA algorithm
rogue routers, 215
role-based access control. See RBAC
roles
  asset classification, 11
  RBAC, 101-103
    best practices, 95
    implementing, 118-122
    management plane, 55
    parser views, 103, 120-122
    privilege levels, customizing, 103, 118-120
  separation of duties, 16
root certificates, 446-448
  authenticating, 450
  installing with SCEP, 457-459
    CA server details, 457
    command line, 458-459
    details, viewing, 459
root certificates

enrollment modes, 458
key pairs, creating, 457
success message, 459
issuers, 447
manually installing, 455-456
public keys, 448
serial numbers, 447
subjects, 447
thumbprint, 448
validity dates, 447
root guards, 192, 228
routers
access authentication, 100
ACS
communication protocols, 141-143
interactions, troubleshooting, 164-170
interoperation, configuring, 142-154
attacks, 213
CCP communication, configuring, 69-70
communities, 70-73
adding devices, 72-73
creating, 71
declared, 71
discovering devices, 73
maximum devices, 71
firewalls. See firewalls
IOS-based IPS
alarm summarization, 392
alerts, 412-416
anti-evasive techniques, 392
benefits, 392
detection methods supported, 392
features, 392
installing from command line, 407-412
installing with CCP, 394-400
regular expression string pattern matching, 392
requirements, 393
response actions, 392
risk ratings, 392
signature files, obtaining, 393-394
signatures. See signatures, IOS-based IPS
threshold configuration, 392
tuning, 412
IOS security features, 228
IPsec
authentication, 471
Diffie-Hellman key exchange, running, 471
encrypting traffic, 472
IKE Phase 1 tunnels, negotiating, 469-470
IKE Phase 2, 471-472
traffic after, 473
traffic before, 472-473
ISR (Integrated Services Routers), 42
on a stick, 182
operating system. See IOS
pinging, 499
rogue, 215
security features, 227-229
AAA, 229
ACLs (packet-filtering), 229
CBAC, 229
control plane protection/policing, 229
IPS, 229
management protocols, 229
reflexive access lists, 229
routing protocol authentication, 229
VPNs, 229
Zone-Based Firewalls, 229
subscriptions, opening, 395
traffic. See traffic
VLANs
inter-VLAN routing, 182
router on a stick, 182
subinterfaces, creating, 182-183
routethrough ASA, 332, 356-357
header 0s, dropping, 215
IPv6, configuring, 208-210
protocols
ACLs, 239
ASA firewalls, 230
control plane, 56
IPv6, 211
routers, 229
RPF (Reverse Path Forwarding), 87
RPO (recovery point objective), 33
RRs (risk ratings), 379-382
calculation factors, 381
factors, 379-382
IOS-based IPS, 392
IPS/IDS actions, 381
RSA (Rivest, Shamir, Adleman)
algorithm, 444
defined, 444
digital signatures, 445, 460
public keys, exchanging, 445
public-private key pairs, 445
RTO (recovery time objective), 33
rule of least privilege, 16
rules
access, storing, 98-99
ACLs, applying, 251
ASA access, 359-362
firewalls
access, 284
guidelines, 285-286
implementation consistency, 286-287
NAT
adding, 357
verifying, 358
PAT, verifying, 358
S
Sarbanes-Oxley (SOX), 28
saving
primary bootset, 132
Security Audit Report Card, 82
user profiles, 80
ScanSafe, 43
SCEP (Simple Certificate Enrollment Protocol), root/identity certificates, installing, 457-459
CA server details, 457
command line, 458-459
details, viewing, 459
enrollment mode, 458
key pairs, creating, 457
success message, 459
scheduler
allocation, 86
intervals, 86
SDEE (Security Device Event Exchange), 385
alerts, delivering, 385
enabling, 395
log file screen
filtering, 414
searching, 414
viewing, 413-414
Search icon (CCP toolbar), 68
Secure Shell. See SSH
Secure Sockets Layer. See SSL
<table>
<thead>
<tr>
<th>术语</th>
<th>描述</th>
</tr>
</thead>
<tbody>
<tr>
<td>secured management protocols</td>
<td>43</td>
</tr>
<tr>
<td>SecureX architecture</td>
<td>42</td>
</tr>
<tr>
<td>AnyConnect Client</td>
<td>42</td>
</tr>
<tr>
<td>context awareness</td>
<td>42</td>
</tr>
<tr>
<td>SIO (Security Intelligence Operations)</td>
<td>42</td>
</tr>
<tr>
<td>TrustSec</td>
<td>42</td>
</tr>
<tr>
<td>Security Audit (CCP)</td>
<td>81</td>
</tr>
<tr>
<td>authentication failure rates</td>
<td>85</td>
</tr>
<tr>
<td>banners, setting</td>
<td>85</td>
</tr>
<tr>
<td>disabling</td>
<td></td>
</tr>
<tr>
<td>BOOTP service, disabling</td>
<td>84</td>
</tr>
<tr>
<td>CDP</td>
<td>84</td>
</tr>
<tr>
<td>Finger service</td>
<td>84</td>
</tr>
<tr>
<td>gratuitous ARPs</td>
<td>85</td>
</tr>
<tr>
<td>ICMP redirects</td>
<td>86</td>
</tr>
<tr>
<td>identification service, disabling</td>
<td>84</td>
</tr>
<tr>
<td>IP directed broadcasts</td>
<td>87</td>
</tr>
<tr>
<td>IP mask reply messages</td>
<td>87</td>
</tr>
<tr>
<td>IP source route</td>
<td>85</td>
</tr>
<tr>
<td>IP unreachable</td>
<td>87</td>
</tr>
<tr>
<td>MOP</td>
<td>87</td>
</tr>
<tr>
<td>proxy ARPs</td>
<td>86</td>
</tr>
<tr>
<td>SNMP</td>
<td>86</td>
</tr>
<tr>
<td>TCP small servers service</td>
<td>84</td>
</tr>
<tr>
<td>UDP small servers service</td>
<td>84</td>
</tr>
<tr>
<td>enabling</td>
<td></td>
</tr>
<tr>
<td>AAA</td>
<td>87</td>
</tr>
<tr>
<td>CEF</td>
<td>85</td>
</tr>
<tr>
<td>firewalls</td>
<td>87</td>
</tr>
<tr>
<td>logging</td>
<td>85</td>
</tr>
<tr>
<td>password encryption</td>
<td>85</td>
</tr>
<tr>
<td>RPF</td>
<td>87</td>
</tr>
<tr>
<td>secret password, setting</td>
<td>86</td>
</tr>
<tr>
<td>SSH</td>
<td>87</td>
</tr>
<tr>
<td>TCP keepalives</td>
<td>85</td>
</tr>
<tr>
<td>Telnet settings</td>
<td>86</td>
</tr>
<tr>
<td>HTTP service/vty lines access class, setting</td>
<td>87</td>
</tr>
<tr>
<td>interface connections</td>
<td>82</td>
</tr>
<tr>
<td>minimum password lengths</td>
<td>85</td>
</tr>
<tr>
<td>One-Step Lockdown</td>
<td>84</td>
</tr>
<tr>
<td>options</td>
<td>81</td>
</tr>
<tr>
<td>potential problems</td>
<td></td>
</tr>
<tr>
<td>fixing</td>
<td>82-83</td>
</tr>
<tr>
<td>identifying</td>
<td>82</td>
</tr>
<tr>
<td>scheduler, setting</td>
<td></td>
</tr>
<tr>
<td>allocation</td>
<td>86</td>
</tr>
<tr>
<td>intervals</td>
<td>86</td>
</tr>
<tr>
<td>starting</td>
<td>81</td>
</tr>
<tr>
<td>summary</td>
<td>83</td>
</tr>
<tr>
<td>TCP SYN-Wait times, setting</td>
<td>85</td>
</tr>
<tr>
<td>users, configuring</td>
<td>86</td>
</tr>
</tbody>
</table>

Security Device Event Exchange. See SDEE

Security Intelligence Operations (SIO), 42, 231, 386

security terms, 10

self zones, 297-298

sensors
<table>
<thead>
<tr>
<th>术语</th>
<th>描述</th>
</tr>
</thead>
<tbody>
<tr>
<td>alerts, delivering</td>
<td>385</td>
</tr>
<tr>
<td>countermeasure actions, 379-380</td>
<td></td>
</tr>
<tr>
<td>deny attacker inline</td>
<td>380</td>
</tr>
<tr>
<td>deny connection inline</td>
<td>380</td>
</tr>
<tr>
<td>deny packet inline</td>
<td>380</td>
</tr>
<tr>
<td>log attacker packets</td>
<td>380</td>
</tr>
<tr>
<td>log pair packets</td>
<td>380</td>
</tr>
<tr>
<td>log victim packets</td>
<td>380</td>
</tr>
<tr>
<td>produce alert</td>
<td>380</td>
</tr>
<tr>
<td>produce verbose alert</td>
<td>380</td>
</tr>
<tr>
<td>request block connection</td>
<td>380</td>
</tr>
<tr>
<td>request block host</td>
<td>380</td>
</tr>
<tr>
<td>request SNMP trap</td>
<td>380</td>
</tr>
<tr>
<td>defined</td>
<td>374</td>
</tr>
</tbody>
</table>
signatures

intelligence
collecting, 385-386
global correlation, 386

IPS/IDS
best practices, 386
comparison, 375-376
malicious traffic, identifying, 377
anomaly-based IPS/IDS, 378
method advantages/disadvantages, 379
policy-based IPS/IDS, 378
reputation-based IPS/IDS, 378-379
signature-based IPS/IDS, 377-378
platforms, 375-376
risk ratings, 379-382
actions, implementing, 381
factors, 379-382

separation of duties, 16
serial numbers (certificates), 447, 449

servers
ACS. See ACS
central, 98-99
DHCP, 355
DNS, 305
SNMP logs, receiving, 104
syslogs, receiving, 104

services
AAA, 55
BOOTP, disabling, 84
Finger, disabling, 84
HTTP access class, configuring, 87
identification, disabling, 84
micro-engine, 384
password encryption, enabling, 85
policies
traffic interaction between zones, 297-298
ZBFs, 297
SIO (Security Intelligence Operations), 231
TCP small servers, disabling, 84
UDP small servers, disabling, 84

SET messages, 129
SFR (signature fidelity rating), 382, 385

signatures
alerts, viewing, 413
certificates, 449
digital, 438
creating, 445
DSA (Digital Signature Algorithm), 444
RSA, 460
VPNs, 435-436

groupings, 384

IOS-based IPS
actions, 405
compiling, 399-400
configuration changes output, 403-404
configuration files, locating, 397
disabling, 401
editing, 401
enabling, 401, 404-405
files, obtaining, 393-394
filtering based on signature IDs, 402
locations, defining, 396
modification buttons, 401
properties, editing, 402, 406
public key, adding, 397
retiring, 401
testing, 406
unretiring, 401
viewing, 400
IPS/IDS, 377-378
 ASR (attack severity rating), 384-385
groups, 384
 micro-engines, 384
 SFR (signature fidelity rating), 385
retired/unretired/enabled/disabled matrix, 384
Simple Network Management Protocol. See SNMP
 single-console management tools, 43
 single root CAs, 453
SIO (Security Intelligence Operations), 42, 231, 386
site-to-site VPNs, 427
crypto policies, configuring, 508-510
digital certificates, 504-505
file sharing needs assessment, 498
IKE Phase 1, 499-500
 authentication, 499
 configuring, 506-507
 Diffie-Hellman key exchange, 499
 encryption, 499
 hashes, 499
 lifetimes, 499
 troubleshooting, 512
IKE Phase 2, 501-502
 configuring, 507-510
 encryption, 501
 hashes, 501
 interfaces, selecting, 501
 lifetimes, 501
 peer IP addresses, 501
 PFS, 501
 traffic encryption, 501
NTP, implementing, 502-504
 configuring, 502
 verifying, 503-504
pinging routers, 499
protocols, 499
SSL VPNs, compared, 532-533
troubleshooting
 configuration, verifying, 511
 IKE Phase 1, 512
 IKE Phase 2, 522-525
 router 1 configuration, 513-515
 router 2 configuration, 517-521
 source interfaces with associated IP addresses, 515-516
 traffic triggers, 512
sniffing (IPv6), 212
SNMP (Simple Network Management Protocol), 56
agent, 128
configuring
 CCP, 130-131
 command line, 131
defined, 128
disabling, 86
logs, receiving, 104
management plane protection, 56
manager, 128
message types, 129
MIB, 128
security levels, 129
security model, 129
sending/receiving information vulnerability, 129
v1/v2 security weaknesses, 129
v3 security
 enhancements, 130
 security levels, 129
social engineering attacks, 15
solicited-node multicast addresses, 207
source IP addresses
   interfaces, testing, 515-516
   NAT, 278-279
SOX (Sarbanes-Oxley), 28
Spanning Tree Protocol. See STP
split tunneling, 554-555
spoofing attacks, preventing, 59
SSH (Secure Shell), 87
   enabling, 87
   implementing, 122-124
SSL (Secure Sockets Layer), 437-438
   AnyConnect VPNs
      AnyConnect client installation, 550
      AnyConnect software packages, choosing, 546-547
      authentication, 547-548
      clientless SSL VPNs, compared, 545
      command line configuration, 550-552
      connection profiles, creating, 545
      digital certificates, 546
      DNS, configuring, 548
      domain name configurations, 548
      groups, 552-553
      IP address pool, assigning, 548
      NAT exemptions, 549
      protocols, choosing, 546
      split tunneling, 554-555
      SSL_AnyConnect connection profile/tunnel group/Group correlation, 553
      summary page, 550
   VPN AnyConnect Wizard, starting, 545
   WINS, configuring, 548
clientless VPNs
   authentication, 538-540
   CLI implementation, 540-541
   configuring on ASA, 535-544
   digital certificates, 537
   interfaces, 537
   logging in, 541
   session details, viewing, 543-544
   SSL VPN Wizard, 535-544
features, 534
   overview, 427
   TLS, compared, 532-534
VPPs
   implementing, 437-438
   IPsec, compared, 532-533
   types, 534
   wizard, 535-544
standard ACLs
   defined, 242
   extended ACLs, compared, 243
   identifying, 242
   IPv4 packet filtering. See IPv4, packet filtering
standards
   defined, 31
   PKCS (Public Key Cryptography Standards), 450, 460
Startup wizard (ASDM), 346-347
stateful filtering, 230, 276-277
   ASA, 331
static NAT, 283
static packet filtering, 274-275
static routes, 356-357
status bar (CCP), 69
Step by Step wizard, 476
storing
   primary bootset, 132
   usernames/passwords/access rules, 98-99

storm control (switches), 228

STP (Spanning Tree Protocol), 183
   loops lifecycle, 184
   new ports, 187
   PVST+, 187
   Rapid Spanning Tree, 187-188
   verification/annotations, 184-187

strategies
   changing nature of networks, 40
   logical boundaries, 40-41
      data centers, 41
      end zones, 41
      Internet, 41
   policy management points, 41
   prevention, 42-43
      ASA firewalls, 42
      IPS (Intrusion Prevention System), 43
      IronPort Email Security/Web Security Appliances, 43
      ISR (Integrated Services Routers), 42
      ScanSafe, 43
   secured management protocols, 43
   SecureX architecture, 42
      AnyConnect Client, 42
      context awareness, 42
      SIO (Security Intelligence Operations), 42
      TrustSec, 42
   single-console management tools, 43
   threat mitigation/containment, 224
      ACLs. See ACLs
      ASA firewalls, 230

CSM (Cisco Security Manager), 231
   end-user education, 226
   end user risks, 224-225
   IPS (Intrusion Prevention System), 231
   mitigation policies/techniques, 226
   opportunities for attacks, 224
   policy procedures, 226
   potential risks, 224
   routers, 227-229
   SIO (Security Intelligence Operations), 231
   switches, 227
   VPN connectivity, 43

stream ciphers, 432

strings
   micro-engine, 384
   pattern matching (regular expressions), 392

study plan, 562

subinterfaces (VLANs), creating, 182-183

subordinate CAs, 453, 460

subscriptions (routers), opening, 395

substitution ciphers, 431

switches
   access ports, assigning, 178-179
   err-disabled ports, restoring, 191-192
   ports
      BPDU guards, 190-191
      locking down, 189-190
   root guards, 192
   security features, 227
      BPDU guards, 228
      DHCP snooping, 228
      dynamic ARP inspections, 228
      IP source guards, 228
modules, 228
port security, 228
root guards, 228
storm control, 228

trunking
  automatic switch negotiation, 182
  native VLANs, 181
  negotiations, not allowing, 190
  security best practices, 189
  security tools, 190
  switch ports, locking down, 189-190
  traffic tags, creating, 180-181

symmetric algorithms, 432-433, 438

syslog
  locking down, 56
  logging, 105
  output, viewing, 127
  receiving, 104
  summary messages, 257
  support, configuring, 125-126
  system files, protecting, 96

Telnet
denial, verifying, 366-367
settings, enabling, 86
templates (CCP), 74-78
  applying, 76-77
  creating, 75-76
  merging/overriding options, 77-78
Terminal Access Control Access Control Server. See TACACS+
test aaa command, 115, 164-165
test preparation tools
  activating/downloading exams, 560
  CD software, installing, 560
  Cisco Learning Network, 561
  memory tables. See memory tables
  Pearson IT Certification Practice Test engine
    modes, 563
    navigating, 563
  practice exams, 559
  Premium Edition practice exams, 561
  videos, 562
testing. See also verifying
  AAA connections, 115
  ASA connections, 345
  IPSec traffic triggers, 512
Packet Tracer, 362-367
  command line, 364-366
  input, configuring, 332-362
  launching, 362
  results, 363-364
  Telnet denial, verifying, 366-367
router-to-ACS
  AAA, 164-165
  connections, 164
  method lists, 166-170
security, 30
source interfaces with associated IP
addresses, 515-516

threats, 14-15
back doors, 15
botnets, 17
covert channels, 17
defined, 9-10
DoS/DDoS, 17
evidence, collecting, 32
incident response policies, 32
IPv6
application layer, 212
DoS attacks, 212
man-in-the-middle attacks, 212
router attacks, 213
spoofed packets, 212
unauthorized access, 212
Layer 2, mitigating
best practices, 189
BPDU guards, 190-191
erd-enabled ports, restoring, 191-192
negotiations, not allowing, 190
port security, 192-194
root guards, 192
switch ports, locking down, 189-190
tools, 190
upper-layer disruptions, 188
malicious traffic
general vulnerabilities, 241
IP address spoofing, 240
reconnaissance attacks, 240-241
risks, reducing. See IPS/IDS
stopping, 239-240
TCP SYN-flood attacks, 240
man-in-the-middle attacks, 14-16
mitigation/containment strategies,
designing, 224
ACLs. See ACLs
application layer visibility, 226
ASA firewalls, 230
centralized monitoring, 226
CSM (Cisco Security Manager), 231
defense in depth, 226
defend user education, 226
def end user risks, 224-225
def incident responses, 226
IPS (Intrusion Prevention System), 231
mitigation policies/techniques, 226
opportunities for attacks, 224
policy procedures, 226
potential risks, 224
routers, 227-229
SIO services, 231
switches, 227
monitoring, 42-43
ASA firewalls, 42
IPS (Intrusion Prevention System), 43
IronPort Email Security/Web Security Appliances, 43
ISR (Integrated Services Routers), 42
ScanSafe, 43
password attacks, 17
pharming, 15
phishing, 15
potential attackers, 13-14
motivations/interests,
understanding, 14
types, 13
privilege escalation, 15
reconnaissance, 15
social engineering, 15
trust exploitation, 17
vectors, 14
thresholds, configuring, 392
thumbprints (certificates), 448-449
time accuracy, 56, 96, 105-106.
See also NTP
timing attacks (IPS/IDS), 381
TLS (Transport Layer Security), 532-534
toolbars (CCP), 67-68
tools
ASAs, 336-337
IPsec, 475
Layer 2 security, 190
traffic
ASA, filtering, 337-338
default flow, 335-336
implementing, 338
inbound, 337-338
outbound traffic, 338
routing, 356-357
encrypting
identifying, 475
IKE Phase 2, planning, 501
IPsec, 472, 480-481
after IPsec, 473
before IPsec, 472-473
fragmentation, 381
inspection direction, choosing, 396
IPsec triggering, testing, 512
malicious
countermeasure actions, 379-380
general vulnerabilities, 241
identifying, 377-379
IP address spoofing, 240
reconnaissance attacks, 240-241
risks, reducing. See IPS/IDS
stopping, 239-240
TCP SYN-flood attacks, 240
management, 94
nontransit, 56
CoPP, 56
CPPr, 56
routing protocol authentication, 56
outbound, 242
sensors, 374
spoofed packets, mitigating, 212
substitution/insertion, 381
transit. See transit traffic
ZBFs, 295
interaction between zones, 297-298
self zones, 297-298
transferring risks to someone else, 13
transform sets, 479
creating, 479
default, 479
selecting, 479
traffic, 56
ACLs, 58
bandwidth management, 59
CAM overflow attacks, 59
DAI, 59
DHCP snooping, 59
DoS attacks, preventing, 59
IOS
firewall support, 58
IPS, 58
IP source guard, 59
IPS (Intrusion Prevention System), 59
MAC address flooding, 59
spoofing attacks, preventing, 59
TCP intercept, 58
unicast reverse path forwarding, 58
unwanted traffic, blocking, 59
Transmission Control Protocol. See TCP
transparent firewalls, 276-278
Transport Layer Security (TLS), 532-534
transposition ciphers, 431
trap messages, 129
troubleshooting
ACS, 164-170
AAA, 164-165
connections, 164
method lists, 166-170
reports, 165-166
IPsec site-to-site VPNs
configuration, verifying, 511
IKE Phase 1, 512
IKE Phase 2, 522-525
router 1 configuration, 513-515
router 2 configuration, 517-521
source interfaces with associated IP addresses, testing, 515-516
traffic triggers, 512
IPv6, 214
true negatives, 377
true positives, 377
trunking
automatic switch negotiation, 182
native VLANs, 181
threats, mitigating
best practices, 189
BPDU guards, 190-191
err-disabled ports, restoring, 191-192
negotiations, not allowing, 190
port security, 192-194
root guards, 192
switch ports, locking down, 189-190
tools, 190
topology, 178
traffic, tagging, 180-181
trust exploitation, 17
TrustSec, 42
tuning IPS, 412
tunneling
IKE Phase 1, 469-470
IKE Phase 2, 471-472
IPsec, troubleshooting, 522-525
IPS/IDS, 381
IPv6, 214-215
split, 554-555
VPN
status, 484
verifying, 486-490
TVR (target value rating), 382
type command, 102
types
centralized servers, 98-99
hashes, 434
IPv6 addresses
all-nodes multicast, 206
all-routers multicast addresses, 206
link local, 206
loopback, 206
multicast, 207
solicited-node multicast, 207
unicast/anycast, 206-207
malicious traffic
general vulnerabilities, 241
IP address spoofing, 240
reconnaissance attacks, 240-241
TCP SYN-flood attacks, 240
potential attackers, 13
security policies, 29-30
  application, 30
e-mail, 30
guideline, 29
network, 30
remote-access, 30
telephony, 30
SNMP messages, 129
SSL, 534
VPNs, 427
  IPsec, 427
  MPLS, 427
  SSL, 427
UDP port 500, 500
UDP port 4500, 500
UDP small servers service, disabling, 84
unauthorized access threats, 212
unauthorized users protection, 271
unicast addresses, 206-207
unretiring signatures, 401
unwanted traffic, blocking, 59
updates (exam), 573-574
  companion website, 573
  print version versus online version, 574
URLs, filtering, 230
uRPF (Unicast Reverse Path Forwarding), 58
users
  accounts
    ACS, 160
    parser views, assigning, 122
ACS router configuration, adding, 153-154
asset classification, 11
authentication
  best practices, 95
  implementing, 108-113
  requiring, 14
  SSL VPNs, 538-540
configuring, 86
educating, 226
groups, creating, 158
names, 345
storing, 98-99
packets, encrypting, 472
profiles, 78-80
  AnyConnect SSL VPN connection, creating, 545
  applying, 80
  creating, 79
  restrictions, 78
  saving, 80
  verifying, 80
risks, 224-225
unauthorized, 271
verifying. See AAA
VPN, 99-100
validity dates (certificates), 447, 449
verifying. See also testing
  AAA, 146-147
  ACL configurations, 254
  ASA connections, 345
data integrity, 428-430, 434
  IPsec, 486-490
  IPsec site-to-site VPNs, 511
    router 1 configuration, 513-515
    router 2 configuration, 517-521
NAT, 322-323, 358
NTP, 503-504
PAT rules, 358
router-to-ACS
    AAA, 164-165
    connections, 164
    method lists, 166-170
STP, 184-187
Telnet denial, 366-367
user profiles (CCP), 80
users. See AAA
ZBFs, 314-315, 319
videos (book CD), 562
viewing
    ACS groups summary, 159
alerts
        command line, 415-416
        IPS Alert Statistics tab, 414
        SDEE log file screen, 413-414
        signatures, 413
certificates, 455
logs, 104, 258
SDEE log file screen, 413-414
signatures, 400
SSL VPN sessions, 543-544
syslog output, 127
views
    creating, 103, 121-122
    implementing, 120-122
    user accounts, assigning, 122
virtual private networks. See VPNs
VLANs (virtual LANs)
    access ports, assigning, 178-179
    frames, following, 181
    interface number associations, 349-350
    inter-VLAN routing, 182
    native, 181
    overview, 178
    physical interfaces disadvantage, 182
    router on a stick, 182
    loop lifecycle, 184
    new ports, 187
    PVST+, 187
    Rapid Spanning Tree, 187-188
    verification/annotations, 184-187
subinterfaces, creating, 182-183
threats, mitigating
    best practices, 189
    BPDU guards, 190-191
    err-disabled ports, restoring, 191-192
    negotiations, not allowing, 190
    port security, 192-194
    root guards, 192
    switch ports, locking down, 189-190
    tools, 190
topology, 178
trunking
    automatic switch negotiation, 182
    native VLANs, 181
    traffic, tagging, 180-181
VPNs
    ACLs, 239
    antireplay functionality, 430
    AnyConnect SSL VPNs
        AnyConnect client installation, 550
        AnyConnect software packages, choosing, 546-547
        authentication, 547-548
        clientless SSL VPNS, compared, 545
        command line configuration, 550-552
        connection profiles, creating, 545
digital certificates, 546
DNS, configuring, 548
domain name configurations, 548

groups, 552-553
IP address pool, assigning, 548
NAT exemptions, 549
protocols, choosing, 546
split tunneling, 554-555
SSL AnyConnect connection profile/tunnel group/Group correlation, 553
summary page, 550
VPN AnyConnect Wizard, starting, 545

WINS, configuring, 548
AnyConnect Wizard, starting, 545
ASA firewalls, 230, 333
authentication, 430, 438
benefits, 427-428
clientless SSL
authentication, 538-540
CLI implementation, 540-541
configuring on ASA, 535-544
digital certificates, 537
interfaces, 537
logging in, 541
session details, viewing, 543-544
SSL VPN Wizard, 536-537

components, 438
confidentiality, 428, 438
connectivity, 43
cryptography, 430
asymmetric, 433, 438
block ciphers, 432
ciphers, 430-431
Diffie-Hellman key exchange, 438
digital signatures, 435-436, 438
hashes, 434
key length, 433

key management, 436
keys, 431
stream ciphers, 432
symmetric, 432-433, 438
data integrity, 428-430, 438
IPsec, configuring, 436-437, 475-484

command line, 482-484
IKE Phase 1 policy, 477-478
local Ethernet information, entering, 477
mirrored VPN for remote peers, 485-486
remote peer information, entering, 477
status, 484
Step by Step wizard, 476
summary, 481
traffic encryption, 480-481
transform sets, 479-480
verification, 486-490

IPsec site-to-site
configuration, verifying, 511
crypto policies, configuring, 508-510
digital certificates, 504-505
file sharing needs assessment, 498
IKE Phase 1, configuring, 506-507
IKE Phase 1, planning, 499-500
IKE Phase 1, troubleshooting, 512
IKE Phase 2, configuring, 507-510
IKE Phase 2, planning, 501-502
IKE Phase 2, troubleshooting, 522-525
NTP, implementing, 502-504
pinging routers, 499
protocols, 499
router 1 configuration, verifying, 513-515
router 2 configuration, verifying, 517-521
source interfaces with associated IP addresses, testing, 515-516
SSL VPNs, compared, 532-533
traffic triggers, testing, 512
overview, 426
remote-access, 427
routers, 229
site-to-site, 427
SSL
implementing, 437-438
IPsec VPNs, compared, 532-533
SSL features, 534
TLS, compared, 532-534
types, 534
types, 427
IPsec, 427
MPLS, 427
SSL, 427
user authentication/authorization, 99-100
vty lines
access class, setting, 87
logs, receiving, 104
vulnerabilities
classifying, 11-12
CVE (Common Vulnerabilities and Exposures) database, 12
defined, 9-10
malicious traffic, 241
NVD (National Vulnerability Database), 12
SNMP, 129

W

websites
Cisco Learning Network, 561
companion, 573
Premium Edition, 561
SIO services, 231
VLAN routing, 182
wildcard masks, 244
WINS (AnyConnect clients), configuring, 548
wireless risk assessment, 27
wizards
ASDM Startup, 346-347
Basic Firewall
CME warning message, 303
DNS, choosing, 305
interface not belonging warning message, 303
interfaces, connecting, 302
security levels, choosing, 304
summary page, 305
untrusted interfaces warning message, 303
welcome screen, 302
IPS Policies, 395
NAT, 319-321
Security Audit
fixing identified potential problems, 82-83
identifying potential problems, 82
interface connections, 82
summary, 83
SSL VPN, 535-544
Step by Step, 476
VPN AnyConnect, 545
X - Y

X.500/X.509v3 certificates, 449, 460

Z

ZBFs (Zone-Based Firewalls), 294
  class maps, 296
  components, configuring, 298-300
  configuring, 300-313
    Basic Firewall wizard welcome screen, 302
    CME warning message, 303
    DNS, choosing, 305
    Firewall wizard page, 301-302
    interface not belonging warning message, 303
    interfaces, connecting, 302
    literal CLI commands, 306-313
    security levels, choosing, 304
    summary page, 305
    untrusted interfaces warning message, 303
  features, 294-295
  monitoring, 314-315

NAT
  configuring with CCP, 319-321
  configuring with command line, 322
  verifying, 322-323
overview, 294
policy maps, 297
  actions, 297
  defined, 296

service policies
  defined, 297
  traffic interaction between zones, 297-298

verifying
  CCP, 314-315
  command line, 315-319
zones
  administrator created, 295
  pairs, 295
  self, 297-298
  traffic interaction between, 298