Contents

Introduction xxvi

Part I Fundamentals of Network Security

Chapter 1 Networking Security Concepts 3

“Do I Know This Already?” Quiz 3

Foundation Topics 6

Understanding Network and Information Security Basics 6
Network Security Objectives 6
Confidentiality, Integrity, and Availability 6
Cost-Benefit Analysis of Security 7
Classifying Assets 8
Classifying Vulnerabilities 10
Classifying Countermeasures 10
What Do We Do with the Risk? 11

Recognizing Current Network Threats 12
Potential Attackers 12
Attack Methods 13
Attack Vectors 14
Man-in-the-Middle Attacks 14
Other Miscellaneous Attack Methods 15

Applying Fundamental Security Principles to Network Design 16
Guidelines 16
Network Topologies 17
Network Security for a Virtual Environment 20
How It All Fits Together 22

Exam Preparation Tasks 23
Review All the Key Topics 23
Complete the Tables and Lists from Memory 23
Define Key Terms 23

Chapter 2 Common Security Threats 25

“Do I Know This Already?” Quiz 25

Foundation Topics 27

Network Security Threat Landscape 27
Distributed Denial-of-Service Attacks 27
Social Engineering Methods 28
Social Engineering Tactics 29
Defenses Against Social Engineering 29
Malware Identification Tools 30
Methods Available for Malware Identification 30
Data Loss and Exfiltration Methods 31
Summary 32
Exam Preparation Tasks 33
Review All the Key Topics 33
Complete the Tables and Lists from Memory 33
Define Key Terms 33

Part II Secure Access

Chapter 3 Implementing AAA in Cisco IOS 35
“Do I Know This Already?” Quiz 35
Foundation Topics 38
Cisco Secure ACS, RADIUS, and TACACS 38
Why Use Cisco ACS? 38
On What Platform Does ACS Run? 38
What Is ISE? 39
Protocols Used Between the ACS and the Router 39
Protocol Choices Between the ACS Server and the Client (the Router) 40
Configuring Routers to Interoperate with an ACS Server 41
Configuring the ACS Server to Interoperate with a Router 51
Verifying and Troubleshooting Router-to-ACS Server Interactions 60
Exam Preparation Tasks 67
Review All the Key Topics 67
Complete the Tables and Lists from Memory 67
Define Key Terms 67
Command Reference to Check Your Memory 67

Chapter 4 Bring Your Own Device (BYOD) 71
“Do I Know This Already?” Quiz 71
Foundation Topics 73
Bring Your Own Device Fundamentals 73
BYOD Architecture Framework 74
BYOD Solution Components 74
Mobile Device Management 76
  MDM Deployment Options 76
  On-Premise MDM Deployment 77
  Cloud-Based MDM Deployment 78
Exam Preparation Tasks 80
Review All the Key Topics 80
Complete the Tables and Lists from Memory 80
Define Key Terms 80

Part III Virtual Private Networks (VPN)

Chapter 5 Fundamentals of VPN Technology and Cryptography 83
“Do I Know This Already?” Quiz 83
Foundation Topics 87
Understanding VPNs and Why We Use Them 87
  What Is a VPN? 87
  Types of VPNs 88
  Two Main Types of VPNs 88
  Main Benefits of VPNs 89
  Confidentiality 89
  Data Integrity 90
  Authentication 90
  Antireplay Protection 90
Cryptography Basic Components 91
  Ciphers and Keys 91
  Ciphers 91
  Keys 92
  Block and Stream Ciphers 92
  Block Ciphers 92
  Stream Ciphers 92
  Symmetric and Asymmetric Algorithms 92
  Symmetric 93
  Asymmetric 93
  Hashes 94
  Hashed Message Authentication Code 95
  Digital Signatures 95
  Digital Signatures in Action 95
  Key Management 96
  Next-Generation Encryption Protocols 97
IPsec and SSL  97
IPsec  97
SSL  98

Public Key Infrastructure  99
Public and Private Key Pairs  99
RSA Algorithm, the Keys, and Digital Certificates  99
Who Has Keys and a Digital Certificate?  100
How Two Parties Exchange Public Keys  100
Creating a Digital Signature  100
Certificate Authorities  100
Root and Identity Certificates  101
Root Certificate  101
Identity Certificate  102
Using the Digital Certificates to Get the Peer’s Public Key  103
X.500 and X.509v3 Certificates  103
Authenticating and Enrolling with the CA  104
Public Key Cryptography Standards  105
Simple Certificate Enrollment Protocol  105
Revoked Certificates  105
Uses for Digital Certificates  106
PKI Topologies  106
Single Root CA  107
Hierarchical CA with Subordinate CAs  107
Cross-Certifying CAs  107

Putting the Pieces of PKI to Work  107
ASA’s Default Certificate  108
Viewing the Certificates in ASDM  108
Adding a New Root Certificate  109
Easier Method for Installing Both Root and Identity Certificates  111

Exam Preparation Tasks  116
Review All the Key Topics  116
Complete the Tables and Lists from Memory  117
Define Key Terms  117
Command Reference to Check Your Memory  117
Chapter 6  
**Fundamentals of IP Security  119**

“Do I Know This Already?” Quiz  119

Foundation Topics  122

IPsec Concepts, Components, and Operations  122

The Goal of IPsec  122

The Internet Key Exchange (IKE) Protocol  123

The Play by Play for IPsec  124

*Step 1: Negotiate the IKEv1 Phase 1 Tunnel*  124

*Step 2: Run the DH Key Exchange*  125

*Step 3: Authenticate the Peer*  126

*What About the User’s Original Packet?*  126

*Leveraging What They Have Already Built*  126

*Now IPsec Can Protect the User’s Packets*  127

*Traffic Before IPsec*  127

*Traffic After IPsec*  127

Summary of the IPsec Story  128

Configuring and Verifying IPsec  129

Tools to Configure the Tunnels  129

Start with a Plan  129

Applying the Configuration  129

Viewing the CLI Equivalent at the Router  137

Completing and Verifying IPsec  139

Exam Preparation Tasks  146

Review All the Key Topics  146

Complete the Tables and Lists from Memory  146

Define Key Terms  146

Command Reference to Check Your Memory  147

Chapter 7  
**Implementing IPsec Site-to-Site VPNs  149**

“Do I Know This Already?” Quiz  149

Foundation Topics  152

Planning and Preparing an IPsec Site-to-Site VPN  152

Customer Needs  152

Planning IKEv1 Phase 1  154

Planning IKEv1 Phase 2  154

Implementing and Verifying an IPsec Site-to-Site VPN in Cisco IOS Devices  155

Troubleshooting IPsec Site-to-Site VPNs in Cisco IOS  164
Chapter 8  Implementing SSL VPNs Using Cisco ASA  203

“Do I Know This Already?” Quiz  203

Foundation Topics  206

Functions and Use of SSL for VPNs  206

Is IPsec Out of the Picture?  206

SSL and TLS Protocol Framework  207

The Play by Play of SSL for VPNs  207

SSL VPN Flavors  208

Configuring Clientless SSL VPNs on ASA  209

Using the SSL VPN Wizard  209

Digital Certificates  211

Accessing the Connection Profile  211

Authenticating Users  211

Logging In  215

Seeing the VPN Activity from the Server  217

Using the Cisco AnyConnect Secure Mobility Client  217

Types of SSL VPNs  218

Configuring the Cisco ASA to Terminate the Cisco AnyConnect Secure Mobility Client Connections  218

Groups, Connection Profiles, and Defaults  225

One Item with Three Different Names  226

Split Tunneling  227

Troubleshooting SSL VPN  228

Troubleshooting SSL Negotiations  228

Troubleshooting AnyConnect Client Issues  228

Initial Connectivity Issues  228

Traffic-Specific Issues  230

Exam Preparation Tasks  231

Review All the Key Topics  231

Complete the Tables and Lists from Memory  231

Define Key Terms  231
Part IV Secure Routing and Switching

Chapter 9 Securing Layer 2 Technologies 233

“Do I Know This Already?” Quiz 233

Foundation Topics 236

VLAN and Trunking Fundamentals 236

What Is a VLAN? 236

Trunking with 802.1Q 238

Following the Frame, Step by Step 239

The Native VLAN on a Trunk 239

So, What Do You Want to Be? (Asks the Port) 239

Inter-VLAN Routing 240

The Challenge of Using Physical Interfaces Only 240

Using Virtual “Sub” Interfaces 240

Spanning-Tree Fundamentals 241

Loops in Networks Are Usually Bad 241

The Life of a Loop 241

The Solution to the Layer 2 Loop 242

STP Is Wary of New Ports 245

Improving the Time Until Forwarding 245

Common Layer 2 Threats and How to Mitigate Them 246

Disrupt the Bottom of the Wall, and the Top Is Disrupted, Too 246

Layer 2 Best Practices 246

Do Not Allow Negotiations 247

Layer 2 Security Toolkit 248

Specific Layer 2 Mitigation for CCNA Security 248

BPDU Guard 248

Root Guard 249

Port Security 250

CDP and LLDP 251

DHCP Snooping 253

Dynamic ARP Inspection 254

Exam Preparation Tasks 257

Review All the Key Topics 257

Complete the Tables and Lists from Memory 258

Review the Port Security Video Included with This Book 258

Define Key Terms 258

Command Reference to Check Your Memory 258
Chapter 10  Network Foundation Protection  261

“Do I Know This Already?” Quiz  261

Foundation Topics  264

Using Network Foundation Protection to Secure Networks  264
   The Importance of the Network Infrastructure  264
   The Network Foundation Protection Framework  264
   Interdependence  265
   Implementing NFP  265

Understanding the Management Plane  266
   First Things First  266
   Best Practices for Securing the Management Plane  267

Understanding the Control Plane  268
   Best Practices for Securing the Control Plane  268

Understanding the Data Plane  270
   Best Practices for Protecting the Data Plane  271
   Additional Data Plane Protection Mechanisms  271

Exam Preparation Tasks  272

Review All the Key Topics  272
Complete the Tables and Lists from Memory  272
Define Key Terms  272

Chapter 11  Securing the Management Plane on Cisco IOS Devices  275

“Do I Know This Already?” Quiz  275

Foundation Topics  278

Securing Management Traffic  278
   Beyond the Blue Rollover Cable  278
   Management Plane Best Practices  278
   Password Recommendations  281
   Using AAA to Verify Users  281
   AAA Components  282
   Options for Storing Usernames, Passwords, and Access Rules  282
   Authorizing VPN Users  283
   Router Access Authentication  284
   The AAA Method List  285
   Role-Based Access Control  286
   Custom Privilege Levels  287
   Limiting the Administrator by Assigning a View  287
Chapter 12  Securing the Data Plane in IPv6  

“Do I Know This Already?” Quiz  

Foundation Topics  

Understanding and Configuring IPv6  

Why IPv6?  

The Format of an IPv6 Address  

Understanding the Shortcuts  

Did We Get an Extra Address?  

IPv6 Address Types  

Configuring IPv6 Routing  

Moving to IPv6  

Developing a Security Plan for IPv6  

Best Practices Common to Both IPv4 and IPv6  

Threats Common to Both IPv4 and IPv6  

The Focus on IPv6 Security  

Exam Preparation Tasks  

Review All the Key Topics  

Complete the Tables and Lists from Memory  

Define Key Terms  

Command Reference to Check Your Memory  

Chapter 12  Securing the Data Plane in IPv6  

“Do I Know This Already?” Quiz  

Foundation Topics  

Understanding and Configuring IPv6  

Why IPv6?  

The Format of an IPv6 Address  

Understanding the Shortcuts  

Did We Get an Extra Address?  

IPv6 Address Types  

Configuring IPv6 Routing  

Moving to IPv6  

Developing a Security Plan for IPv6  

Best Practices Common to Both IPv4 and IPv6  

Threats Common to Both IPv4 and IPv6  

The Focus on IPv6 Security  

Exam Preparation Tasks  

Review All the Key Topics  

Complete the Tables and Lists from Memory  

Define Key Terms  

Command Reference to Check Your Memory
New Potential Risks with IPv6 334
IPv6 Best Practices 336
IPv6 Access Control Lists 337
Exam Preparation Tasks 338
Review All the Key Topics 338
Complete the Tables and Lists from Memory 338
Define Key Terms 338
Command Reference to Check Your Memory 338

Chapter 13  Securing Routing Protocols and the Control Plane 341
“Do I Know This Already?” Quiz 341
Foundation Topics 344
Securing the Control Plane 344
Minimizing the Impact of Control Plane Traffic on the CPU 344
Control Plane Policing 346
Control Plane Protection 348
Securing Routing Protocols 348
Implement Routing Update Authentication on OSPF 348
Implement Routing Update Authentication on EIGRP 349
Implement Routing Update Authentication on RIP 350
Implement Routing Update Authentication on BGP 351
Exam Preparation Tasks 353
Review All the Key Topics 353
Complete the Tables and Lists from Memory 353
Define Key Terms 353

Part V  Cisco Firewall Technologies and Intrusion Prevention System Technologies

Chapter 14  Understanding Firewall Fundamentals 355
“Do I Know This Already?” Quiz 355
Foundation Topics 358
Firewall Concepts and Technologies 358
Firewall Technologies 358
Objectives of a Good Firewall 358
Firewall Justifications 359
The Defense-in-Depth Approach 360
Firewall Methodologies 361
Static Packet Filtering 362
Application Layer Gateway 363
Chapter 16  Configuring Basic Firewall Policies on Cisco ASA  413

“Do I Know This Already?” Quiz  413

Foundation Topics  416

The ASA Appliance Family and Features  416
  Meet the ASA Family  416
  ASA Features and Services  417

ASA Firewall Fundamentals  419
  ASA Security Levels  419
  The Default Flow of Traffic  420
  Tools to Manage the ASA  422
  Initial Access  422
  Packet Filtering on the ASA  422
  Implementing a Packet-Filtering ACL  423
  Modular Policy Framework  424
  Where to Apply a Policy  425

Configuring the ASA  425
  Beginning the Configuration  425
  Getting to the ASDM GUI  433
  Configuring the Interfaces  435
  IP Addresses for Clients  443
  Basic Routing to the Internet  444
  NAT and PAT  445
  Permitting Additional Access Through the Firewall  447
  Using Packet Tracer to Verify Which Packets Are Allowed  449
  Verifying the Policy of No Telnet  453

Exam Preparation Tasks  454

Review All the Key Topics  454

Complete the Tables and Lists from Memory  454

Define Key Terms  454

Command Reference to Check Your Memory  455
Chapter 17 Cisco IDS/IPS Fundamentals 457

“Do I Know This Already?” Quiz 457

Foundation Topics 460
IPS Versus IDS 460
What Sensors Do 460
Difference Between IPS and IDS 460
Sensor Platforms 462
True/False Negatives/Positives 463
Positive/Negative Terminology 463
Identifying Malicious Traffic on the Network 463
Signature-Based IPS/IDS 464
Policy-Based IPS/IDS 464
Anomaly-Based IPS/IDS 464
Reputation-Based IPS/IDS 464
When Sensors Detect Malicious Traffic 465
Controlling Which Actions the Sensors Should Take 467
Implementing Actions Based on the Risk Rating 468
Circumventing an IPS/IDS 468
Managing Signatures 469
Signature or Severity Levels 470
Monitoring and Managing Alarms and Alerts 471
Security Intelligence 471
IPS/IDS Best Practices 472
Cisco Next-Generation IPS Solutions 472
Exam Preparation Tasks 474
Review All the Key Topics 474
Complete the Tables and Lists from Memory 474
Define Key Terms 474

Part VI Content and Endpoint Security

Chapter 18 Mitigation Technologies for E-mail-Based and Web-Based Threats 477

“Do I Know This Already?” Quiz 477

Foundation Topics 479
Mitigation Technology for E-mail-Based Threats 479
E-mail-Based Threats 479
Cisco Cloud E-mail Security 479
Cisco Hybrid E-mail Security 480
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, we did so 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, we 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 CCNA Security Implementing Cisco Network Security (IINS) 210-260 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 CCNA Security Implementing Cisco Network Security (IINS) 210-260 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
Introduction

- 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 (VPNs) 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/

**CCNA Security Exam**

Table I-1 lists the topics of the CCNA Security 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>1.0 Security Concepts</strong></td>
<td></td>
</tr>
<tr>
<td>1.1 Common Security Principles</td>
<td></td>
</tr>
<tr>
<td>1.1.a Describe Confidentiality, Integrity, Availability (CIA)</td>
<td>Chapter 1</td>
</tr>
<tr>
<td>1.1.b Describe SIEM technology</td>
<td>Chapter 1</td>
</tr>
<tr>
<td>1.1.c Identify common security terms</td>
<td>Chapter 1</td>
</tr>
<tr>
<td>1.1.d Identify common network security zones</td>
<td>Chapter 1</td>
</tr>
<tr>
<td>1.2 Common Security Threats</td>
<td></td>
</tr>
<tr>
<td>1.2.a Identify Common network attacks</td>
<td>Chapter 2</td>
</tr>
<tr>
<td>1.2.b Describe Social Engineering</td>
<td>Chapter 2</td>
</tr>
<tr>
<td>1.2.c Identify Malware</td>
<td>Chapter 2</td>
</tr>
<tr>
<td>1.2.d Classify the vectors of Data Loss/Exfiltration</td>
<td>Chapter 2</td>
</tr>
<tr>
<td>1.3 Cryptography Concepts</td>
<td></td>
</tr>
<tr>
<td>1.3.a Describe Key Exchange</td>
<td>Chapter 5</td>
</tr>
<tr>
<td>1.3.b Describe Hash Algorithm</td>
<td>Chapter 5</td>
</tr>
<tr>
<td>1.3.c Compare &amp; Contrast Symmetric and Asymmetric Encryption</td>
<td>Chapter 5</td>
</tr>
<tr>
<td>1.3.d Describe Digital Signatures, Certificates and PKI</td>
<td>Chapter 5</td>
</tr>
<tr>
<td>1.4 Describe network topologies</td>
<td></td>
</tr>
<tr>
<td>1.4.a Campus Area Network (CAN)</td>
<td>Chapter 1</td>
</tr>
<tr>
<td>1.4.b Cloud, Wide Area Network (WAN)</td>
<td>Chapter 1</td>
</tr>
<tr>
<td>1.4.c Data Center</td>
<td>Chapter 1</td>
</tr>
<tr>
<td>1.4.d Small office/Home office (SOHO)</td>
<td>Chapter 1</td>
</tr>
<tr>
<td>1.4.e Network security for a virtual environment</td>
<td>Chapter 1</td>
</tr>
<tr>
<td><strong>2.0 Secure Access</strong></td>
<td></td>
</tr>
<tr>
<td>2.1 Secure management</td>
<td></td>
</tr>
<tr>
<td>2.1.a Compare In-band and out of band</td>
<td>Chapter 11</td>
</tr>
<tr>
<td>2.1.b Configure secure network management</td>
<td>Chapter 11</td>
</tr>
<tr>
<td>2.1.c Configure and verify secure access through SNMP v3 using an ACL</td>
<td>Chapter 11</td>
</tr>
<tr>
<td>2.1.d Configure and verify security for NTP</td>
<td>Chapter 11</td>
</tr>
<tr>
<td>2.1.e Use SCP for file transfer</td>
<td>Chapter 11</td>
</tr>
<tr>
<td>Exam Topic</td>
<td>Part</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>2.2 AAA Concepts</td>
<td></td>
</tr>
<tr>
<td>2.2.a Describe RADIUS &amp; TACACS+ technologies</td>
<td>Chapter 3</td>
</tr>
<tr>
<td>2.2.b Configure administrative access on a Cisco router using TACACS+</td>
<td>Chapter 3</td>
</tr>
<tr>
<td>2.2.c Verify connectivity on a Cisco router to a TACACS+ server</td>
<td>Chapter 3</td>
</tr>
<tr>
<td>2.2.d Explain the integration of Active Directory with AAA</td>
<td>Chapter 3</td>
</tr>
<tr>
<td>2.2.e Describe Authentication &amp; Authorization using ACS and ISE</td>
<td>Chapter 3</td>
</tr>
<tr>
<td>2.3. 802.1X Authentication</td>
<td></td>
</tr>
<tr>
<td>2.3.a Identify the functions 802.1X components</td>
<td>Chapter 4</td>
</tr>
<tr>
<td>2.4. BYOD</td>
<td></td>
</tr>
<tr>
<td>2.4.a Describe the BYOD architecture framework</td>
<td>Chapter 4</td>
</tr>
<tr>
<td>2.4.b Describe the function of Mobile Device Management (MDM)</td>
<td>Chapter 4</td>
</tr>
<tr>
<td>3. VPN</td>
<td></td>
</tr>
<tr>
<td>3.1. VPN Concepts</td>
<td></td>
</tr>
<tr>
<td>3.1.a Describe IPSec Protocols and Delivery Modes (IKE, ESP, AH, Tunnel mode, Transport mode)</td>
<td>Chapter 6</td>
</tr>
<tr>
<td>3.1.b Describe Hairpinning, Split Tunneling, Always-on, NAT Traversal</td>
<td>Chapter 6</td>
</tr>
<tr>
<td>3.2. Remote Access VPN</td>
<td></td>
</tr>
<tr>
<td>3.2.a Implement basic Clientless SSL VPN using ASDM</td>
<td>Chapter 8</td>
</tr>
<tr>
<td>3.2.b Verify clientless connection</td>
<td>Chapter 8</td>
</tr>
<tr>
<td>3.2.c Implement basic AnyConnect SSL VPN using ASDM</td>
<td>Chapter 8</td>
</tr>
<tr>
<td>3.2.d Verify AnyConnect connection</td>
<td>Chapter 8</td>
</tr>
<tr>
<td>3.2.e Identify Endpoint Posture Assessment</td>
<td>Chapter 8</td>
</tr>
<tr>
<td>3.3 Site-to-Site VPN</td>
<td></td>
</tr>
<tr>
<td>3.3.a Implement an IPSec site-to-site VPN with pre-shared key authentication on Cisco routers and ASA firewalls</td>
<td>Chapter 7</td>
</tr>
<tr>
<td>3.3.b Verify an IPSec site-to-site VPN</td>
<td>Chapter 7</td>
</tr>
<tr>
<td>4.0. Secure Routing &amp; Switching</td>
<td></td>
</tr>
<tr>
<td>4.1 Security on Cisco Routers</td>
<td></td>
</tr>
<tr>
<td>4.1.a Configure multiple privilege levels</td>
<td>Chapter 11</td>
</tr>
<tr>
<td>4.1.b Configure IOS Role-based CLI Access</td>
<td>Chapter 11</td>
</tr>
<tr>
<td>4.1.c Implement IOS Resilient Configuration</td>
<td>Chapter 11</td>
</tr>
<tr>
<td>Exam Topic</td>
<td>Part</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>4.2 Securing Routing Protocols</td>
<td></td>
</tr>
<tr>
<td>4.2.a Implement routing update authentication on OSPF</td>
<td>Chapter 13</td>
</tr>
<tr>
<td>4.3 Securing the Control Plane</td>
<td></td>
</tr>
<tr>
<td>4.3.a Explain the function of Control Plane Policing</td>
<td>Chapter 13</td>
</tr>
<tr>
<td>4.4 Common Layer 2 Attacks</td>
<td></td>
</tr>
<tr>
<td>4.4.a Describe STP attacks</td>
<td>Chapter 9</td>
</tr>
<tr>
<td>4.4.b Describe ARP Spoofing</td>
<td>Chapter 9</td>
</tr>
<tr>
<td>4.4.c Describe MAC spoofing</td>
<td>Chapter 9</td>
</tr>
<tr>
<td>4.4.d Describe CAM Table (MAC Address Table) Overflows</td>
<td>Chapter 9</td>
</tr>
<tr>
<td>4.4.e Describe CDP/LLDP Reconnaissance</td>
<td>Chapter 9</td>
</tr>
<tr>
<td>4.4.f Describe VLAN Hopping</td>
<td>Chapter 9</td>
</tr>
<tr>
<td>4.4.g Describe DHCP Spoofing</td>
<td>Chapter 9</td>
</tr>
<tr>
<td>4.5 Mitigation Procedures</td>
<td></td>
</tr>
<tr>
<td>4.5.a Implement DHCP Snooping</td>
<td>Chapter 9</td>
</tr>
<tr>
<td>4.5.b Implement Dynamic ARP Inspection</td>
<td>Chapter 9</td>
</tr>
<tr>
<td>4.5.c Implement Port Security</td>
<td>Chapter 9</td>
</tr>
<tr>
<td>4.5.d Describe BPDU Guard, Root Guard, Loop Guard</td>
<td>Chapter 9</td>
</tr>
<tr>
<td>4.5.e Verify mitigation procedures</td>
<td>Chapter 9</td>
</tr>
<tr>
<td>4.6 VLAN Security</td>
<td></td>
</tr>
<tr>
<td>4.6.a Describe the security implications of a PVLAN</td>
<td>Chapter 9</td>
</tr>
<tr>
<td>4.6.b Describe the security implications of a Native VLAN</td>
<td>Chapter 9</td>
</tr>
<tr>
<td>5.0 Cisco Firewall Technologies</td>
<td></td>
</tr>
<tr>
<td>5.1 Describe operational strengths and weaknesses of the different firewall technologies</td>
<td>Chapter 14</td>
</tr>
<tr>
<td>5.1.a Proxy firewalls</td>
<td>Chapter 14</td>
</tr>
<tr>
<td>5.1.b Application firewall</td>
<td>Chapter 14</td>
</tr>
<tr>
<td>5.1.c Personal firewall</td>
<td>Chapter 14</td>
</tr>
<tr>
<td>5.2 Compare Stateful vs. Stateless Firewalls</td>
<td></td>
</tr>
<tr>
<td>5.2.a Operations</td>
<td>Chapter 16</td>
</tr>
<tr>
<td>5.2.b Functions of the state table</td>
<td>Chapter 16</td>
</tr>
<tr>
<td>Exam Topic</td>
<td>Part</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td><strong>5.3 Implement NAT on Cisco ASA 9.x</strong></td>
<td></td>
</tr>
<tr>
<td>5.3.a Static</td>
<td>Chapter 16</td>
</tr>
<tr>
<td>5.3.b Dynamic</td>
<td>Chapter 16</td>
</tr>
<tr>
<td>5.3.c PAT</td>
<td>Chapter 16</td>
</tr>
<tr>
<td>5.3.d Policy NAT</td>
<td>Chapter 16</td>
</tr>
<tr>
<td>5.3 e Verify NAT operations</td>
<td>Chapter 16</td>
</tr>
<tr>
<td><strong>5.4 Implement Zone Based Firewall</strong></td>
<td></td>
</tr>
<tr>
<td>5.4.a Zone to zone</td>
<td>Chapter 15</td>
</tr>
<tr>
<td>5.4.b Self zone</td>
<td>Chapter 15</td>
</tr>
<tr>
<td><strong>5.5 Firewall features on the Cisco Adaptive Security Appliance (ASA) 9.x</strong></td>
<td></td>
</tr>
<tr>
<td>5.5.a Configure ASA Access Management</td>
<td>Chapter 16</td>
</tr>
<tr>
<td>5.5.b Configure Security Access Policies</td>
<td>Chapter 16</td>
</tr>
<tr>
<td>5.5.c Configure Cisco ASA interface security levels</td>
<td>Chapter 16</td>
</tr>
<tr>
<td>5.5.d Configure Default Modular Policy Framework (MPF)</td>
<td>Chapter 16</td>
</tr>
<tr>
<td>5.5.e Describe Modes of deployment (Routed firewall, Transparent firewall)</td>
<td>Chapter 16</td>
</tr>
<tr>
<td>5.5.f Describe methods of implementing High Availability</td>
<td>Chapter 16</td>
</tr>
<tr>
<td>5.5.g Describe Security contexts</td>
<td>Chapter 16</td>
</tr>
<tr>
<td>5.5.h Describe Firewall Services</td>
<td>Chapter 16</td>
</tr>
<tr>
<td><strong>6.0 IPS</strong></td>
<td></td>
</tr>
<tr>
<td>6.1 Describe IPS Deployment Considerations</td>
<td>Chapter 17</td>
</tr>
<tr>
<td>6.1.a Network Based IPS vs. Host Based IPS</td>
<td>Chapter 17</td>
</tr>
<tr>
<td>6.1.b Modes of deployment (Inline, Promiscuous - SPAN, tap)</td>
<td>Chapter 17</td>
</tr>
<tr>
<td>6.1.c Placement (positioning of the IPS within the network)</td>
<td>Chapter 17</td>
</tr>
<tr>
<td>6.1.d False Positives, False Negatives, True Positives, True Negatives</td>
<td>Chapter 17</td>
</tr>
<tr>
<td>6.2 Describe IPS Technologies</td>
<td></td>
</tr>
<tr>
<td>6.2.a Rules/Signatures</td>
<td>Chapter 17</td>
</tr>
<tr>
<td>6.2.b Detection/Signature Engines</td>
<td>Chapter 17</td>
</tr>
<tr>
<td>6.2.c Trigger Actions/Responses (drop, reset, block, alert, monitor/log, shun)</td>
<td>Chapter 17</td>
</tr>
<tr>
<td>6.2.d Blacklist (Static &amp; Dynamic)</td>
<td>Chapter 17</td>
</tr>
</tbody>
</table>
Exam Topic | Part
---|---
7.0 Content and Endpoint Security | Chapter 18
7.1 Describe Mitigation Technology for Email-based Threats | Chapter 18
7.1.a SPAM Filtering, Anti-Malware Filtering, DLP, Blacklisting, Email Encryption | Chapter 18
7.2 Describe Mitigation Technology for Web-based Threats | Chapter 18
7.2.a Local & Cloud Based Web Proxies | Chapter 18
7.2.b Blacklisting, URL-Filtering, Malware Scanning, URL Categorization, Web Application Filtering, TLS/SSL Decryption | Chapter 18
7.3 Describe Mitigation Technology for Endpoint Threats | Chapter 19
7.3.a Anti-Virus/Anti-Malware | Chapter 19
7.3.b Personal Firewall/HIPS | Chapter 19
7.3.c Hardware/Software Encryption of local data | Chapter 19

About the CCNA Security 210-260 Official Cert Guide

This book maps to the topic areas of the CCNA Security 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 19 core chapters. Chapter 20 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, “Common Security Threats”: This chapter covers the current state of network security in terms of the types of threats organizations face on behalf of malicious actors. It provides coverage of different threat landscape topics and common attacks such as distributed denial-of-service (DDoS) attacks, social engineering, malware identification tools, data loss, and exfiltration.

Part II: Secure Access

Chapter 3, “Implementing AAA in Cisco IOS”: This chapter covers the role of Cisco Secure ACS and the Cisco Identity Services Engine (ISE), along with the two primary protocols used for authentication 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 4, “Bring Your Own Device (BYOD)”: This chapter covers different subjects focused on the topic of BYOD. It provides a description of the BYOD concept and an overview of a BYOD architecture framework. This chapter covers the fundamentals of mobile device management (MDM), its function, and the deployment options.

Part III: Virtual Private Networks (VPN)

Chapter 5, “Fundamentals of VPN Technology and Cryptography”: This chapter covers what VPNs are and why we use them and the basic ingredients of cryptography. This chapter also 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 6, “Fundamentals of IP Security”: This chapter covers the concepts, components, and operations of IPsec and how to configure and verify IPsec.

Chapter 7, “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 8, “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.

Part IV: Secure Routing and Switching

Chapter 9, “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 10, “Network Foundation Protection”: This chapter covers securing the network using the network foundation protection (NFP) approach, the management plane, the control plane, and the data plane.

Chapter 11, “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 12, “Securing the Data Plane in IPv6”: This chapter covers IPv6 (basics, configuring, and developing a security plan for IPv6).
Chapter 13, “Securing Routing Protocols and the Control Plane”: This chapter covers different subjects focused on the control plane of the network device. It provides details on how to secure the control plane of network infrastructure devices. This chapter explains the function of control plane policing (CoPP), control plane protection (CPPr), and how to secure IP routing protocols.

Part V: Cisco Firewall Technologies and Intrusion Prevention System Technologies

Chapter 14, “Understanding Firewall Fundamentals”: This chapter covers firewall concepts and the technologies used by them, the function of Network Address Translation (NAT), including its building blocks, and the guidelines and considerations for creating and deploying firewalls.

Chapter 15, “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 16, “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 17, “Cisco IPS 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.

Part VI: Content and Endpoint Security

Chapter 18, “Mitigation Technologies for E-Mail-Based and Web-Based Threats”: This chapter covers the different mitigation technologies for e-mail-based and web-based threats. It covers the Cisco Email Security Appliances (ESA), Cisco cloud e-mail security, Cisco Cloud Web Security (CWS), the Cisco Web Security Appliance (WSA), and the Cisco Content Security Management Appliance (SMA). Cisco has added advanced malware protection (AMP) to the ESA and WSA to enable security administrators to detect and block malware and perform continuous analysis and retrospective alerting. Both the ESA and WSA use cloud-based security intelligence to allow protection before, during, and after an attack. This chapter covers these technologies and solutions in detail. It details mitigation technologies such as spam and antimalware filtering, data loss prevention (DLP), blacklisting, e-mail encryption, and web application filtering.

Chapter 19, “Mitigation Technology for Endpoint Threats”: This chapter provides details of the different mitigation technologies available for endpoint threats. It covers introductory concepts of endpoint threats to advanced malware protection capabilities provided by Cisco security products. This chapter covers the different antivirus and antimalware solutions, personal firewalls and host intrusion prevention systems (HIPS), Cisco AMP for endpoints, and hardware and software encryption of endpoint data.

Part VII: Final Preparation

Chapter 20, “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 19.
- Appendix B, “CCNA Security 210-260 (IINS) Exam Updates”: This appendix provides instructions for finding updates to the exam and this book when and if they occur.
- Glossary: The glossary contains definitions for all the terms listed in the “Define Key Terms” sections at the conclusions of Chapters 1 through 19.

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.
- Appendix E, “Study Planner”: This spreadsheet provides major study milestones where you can track your progress through your study.
- Glossary: The glossary contains definitions for all the terms listed in the “Define Key Terms” sections at the conclusions of Chapters 1 through 19.

Premium Edition eBook and Practice Test

This Cert Guide contains a special offer for a 70 percent discount off the companion CCNA Security 210-260 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 need the coupon code included on the paper in the CD sleeve. Just follow the purchasing instructions that accompany the code to download and start using your Premium Edition today.
This chapter covers the following topics:

- Mitigation technology for e-mail-based threats
- Mitigation technology for web-based threats
CHAPTER 18

Mitigation Technologies for E-mail-Based and Web-Based Threats

Efficient e-mail-based and web-based security requires a robust solution that is expanded beyond the traditional perimeter, as new threats are emerging on a daily basis. The Cisco E-mail Security Appliances (ESA) and the Cisco Web Security Appliance (WSA) provide a great solution designed to protect corporate users against these threats. Cisco has added advanced malware protection (AMP) to the ESA and WSA to allow security administrators to detect and block malware and perform continuous analysis and retrospective alerting. Both the ESA and WSA use cloud-based security intelligence to allow protection before, during, and after an attack. This chapter covers these technologies and solutions in detail.

You will learn mitigation technologies such as spam and antimalware filtering, data loss prevention (DLP), blacklisting, e-mail encryption, and web application filtering.

“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 18-1 details the major topics discussed in this chapter and their corresponding quiz questions.

Table 18-1   “Do I Know This Already?” Section-to-Question Mapping

<table>
<thead>
<tr>
<th>Foundation Topics Section</th>
<th>Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mitigation Technology for E-mail-Based Threats</td>
<td>1–4</td>
</tr>
<tr>
<td>Mitigation Technology for Web-Based Threats</td>
<td>5–8</td>
</tr>
</tbody>
</table>

1. Which of the following features does the Cisco ESA provide? (Choose all that apply.)
   a. Network antivirus capabilities
   b. E-mail encryption
   c. Threat outbreak prevention
   d. Support for remote access SSL VPN connections

2. Which of the following Cisco ESA models are designed for mid-sized organizations? (Choose all that apply.)
   a. Cisco C380
   b. Cisco C670
   c. Cisco C680
   d. Cisco X1070
3. What is a spear phishing attack?
   a. Unsolicited e-mails sent to an attacker.
   b. A denial-of-service (DoS) attack against an e-mail server.
   c. E-mails that are directed to specific individuals or organizations. An attacker may obtain information about the targeted individual or organization from social media sites and other sources.
   d. Spam e-mails sent to numerous victims with the purpose of making money.

4. Which of the following e-mail authentication mechanisms are supported by the Cisco ESA? (Choose all that apply.)
   a. Sender Policy Framework (SPF)
   b. Sender ID Framework (SIDF)
   c. DomainKeys Identified Mail (DKIM)
   d. DomainKeys Mail Protection (DMP)

5. Which of the following is the operating system used by the Cisco WSA?
   a. Cisco AsyncOS operating system
   b. Cisco IOS-XR Software
   c. Cisco IOS-XE Software
   d. Cisco IOS Software
   e. Cisco ASA Software

6. Which of the following connectors are supported by the Cisco CWS service? (Choose all that apply.)
   a. Cisco Security Manager (CSM)
   b. Cisco ASA
   c. Cisco ISR G2 routers
   d. Cisco AnyConnect Secure Mobility Client
   e. Cisco WSA

7. Which of the following features are supported by the Cisco WSA? (Choose all that apply.)
   a. File reputation
   b. File sandboxing
   c. Layer 4 traffic monitor
   d. Real-time e-mail scanning
   e. Third-party DLP integration

8. Cisco WSA can be deployed using the Web Cache Communication Protocol (WCCP) configured in which of the following modes? (Choose all that apply.)
   a. Multiple context mode
   b. Explicit proxy mode
   c. Transparent proxy mode
   d. Virtualized mode
Foundation Topics

Mitigation Technology for E-mail-Based Threats

Users are no longer accessing e-mail from the corporate network or from a single device. Cisco provides cloud-based, hybrid, and on-premises ESA-based solutions that can help protect any dynamic environment. This section introduces these solutions and technologies explaining how users can use threat intelligence to detect, analyze, and protect against both known and emerging threats.

E-mail-Based Threats

There are several types of e-mail-based threats. The following are the most common:

- **Spam**: Unsolicited e-mail messages that can be advertising a service or (typically) a scam or a message with malicious intent. E-mail spam continuous to be a major threat because it can be used to spread malware.

- **Malware attachments**: E-mail messages containing malicious software (malware).

- **Phishing**: An attacker’s attempt to fool a user that such e-mail communication comes from a legitimate entity or site, such as banks, social media websites, online payment processors, or even corporate IT communications. The goal of the phishing e-mail is to steal user’s sensitive information such as user credentials, bank accounts, and so on.

- **Spear phishing**: Phishing attempts that are more targeted. These phishing e-mails are directed to specific individuals or organizations. For instance, an attacker may perform a passive reconnaissance on the individual or organization by gathering information from social media sites (for example, Twitter, LinkedIn, Facebook) and other online resources. Then the attacker may tailor a more directed and relevant message to the victim increasing the probability of such user being fooled to follow a malicious link, click an attachment containing malware, or simply reply to the e-mail providing sensitive information. There is another phishing-based attack called *whaling*. These attacks specifically target executives and high-profile users within a given organization.

Cisco Cloud E-mail Security

Cisco cloud e-mail security provides a cloud-based solution that allows companies to outsource the management of their e-mail security management. The service provides e-mail security instances in multiple Cisco data centers to enable high availability. Figure 18-1 illustrates the Cisco cloud e-mail security solution.

In Figure 18-1, three organizations (a large enterprise, a university, and a small- to medium-size business) leverage the Cisco hosted (cloud) environment. The solution also supports mobile workers.
Cisco Hybrid E-mail Security

The Cisco hybrid e-mail security solution combines both cloud-based and on-premises ESAs. This hybrid solution helps Cisco customers reduce their on-site e-mail security footprint, outsourcing a portion of their e-mail security to Cisco, while still allowing them to maintain control of confidential information within their physical boundaries. Many organizations need to stay compliant to many regulations that may require them to keep sensitive data physically on their premises. The Cisco hybrid e-mail security solution allows network security administrators to remain compliant and to maintain advanced control with encryption, data loss prevention (DLP), and on-site identity-based integration.

Cisco E-mail Security Appliance

The following are the different ESA models:

- Cisco X-Series E-mail Security Appliances
  - Cisco X1070: High-performance ESA for service providers and large enterprises
- Cisco C-Series E-mail Security Appliances
  - Cisco C680: The high-performance ESA for service providers and large enterprises
  - Cisco C670: Designed for medium-size enterprises
  - Cisco C380: Designed for medium-size enterprises
  - Cisco C370: Designed for small- to medium-size enterprises
  - Cisco C170: Designed for small businesses and branch offices
The Cisco ESA runs the Cisco AsyncOS operating system. The Cisco AsyncOS supports numerous features that will help mitigate e-mail-based threats. The following are examples of the features supported by the Cisco ESA:

- **Access control:** Controlling access for inbound senders according to the sender’s IP address, IP address range, or domain name.
- **Antispam:** Multilayer filters based on Cisco SenderBase reputation and Cisco antispam integration. The antispam reputation and zero-day threat intelligence are fueled by Cisco’s security intelligence and research group named Talos.
- **Network Antivirus:** Network antivirus capabilities at the gateway. Cisco partnered with Sophos and McAfee, supporting their antivirus scanning engines.
- **Advanced malware protection (AMP):** Allows security administrators to detect and block malware and perform continuous analysis and retrospective alerting.
- **DLP:** The ability to detect any sensitive e-mails and documents leaving the corporation. The Cisco ESA integrates RSA e-mail DLP for outbound traffic.

**NOTE** If RSA e-mail DLP is configured on a Cisco ESA that is also running antispam and antivirus scanning on inbound traffic, it can cause a performance decrease of less than 10 percent. Cisco ESAs that are only running outbound messages and are not running antispam and antivirus may experience a significant performance decline.

- **E-mail encryption:** The ability to encrypt outgoing mail to address regulatory requirements. The administrator can configure an encryption policy on the Cisco ESA and use a local key server or hosted key service to encrypt the message.
- **E-mail authentication:** A few e-mail authentication mechanisms are supported, including Sender Policy Framework (SPF), Sender ID Framework (SIDF), and DomainKeys Identified Mail (DKIM) verification of incoming mail, as well as DomainKeys and DKIM signing of outgoing mail.
- **Outbreak filters:** Preventive protection against new security outbreaks and e-mail-based scams using Cisco’s Security Intelligence Operations (SIO) threat intelligence information.

**NOTE** Cisco SenderBase is the world largest e-mail and web traffic monitoring network. It provides real-time threat intelligence powered by Cisco Security Intelligence Operations (SIO). The Cisco SenderBase website is located at http://www.senderbase.org.

The Cisco ESA acts as the e-mail gateway to the organization, handling all e-mail connections, accepting messages, and relaying them to the appropriate systems. The Cisco ESA can service e-mail connections from the Internet to users inside your network, and from systems inside your network to the Internet. E-mail connections use Simple Mail Transfer Protocol (SMTP). The ESA services all SMTP connections by default acting as the SMTP gateway.
NOTE Mail gateways are also known as a mail exchangers or MX.

The Cisco ESA uses listeners to handle incoming SMTP connection requests. A listener defines an e-mail processing service that is configured on an interface in the Cisco ESA. Listeners apply to e-mail entering the appliance from either the Internet or from internal systems.

The following listeners can be configured:
- Public listeners for e-mail coming in from the Internet.
- Private listeners for e-mail coming from hosts in the corporate (inside) network. These e-mails are typically from an internal groupware, Exchange, POP, or IMAP e-mail servers.

Figure 18-2 illustrates the concept of Cisco ESA listeners.

![Figure 18-2 Cisco ESA Listeners](image)

Cisco ESA listeners are often referred to as SMTP daemons running on a specific Cisco ESA interface. When a listener is configured, the following information must be provided:
- Listener properties such as a specific interface in the Cisco ESA and the TCP port that will be used. The listener properties must also indicate whether it is a public or a private listener.
- The hosts that are allowed to connect to the listener using a combination of access control rules. An administrator can specify which remote hosts can connect to the listener.
- The local domains for which public listeners accept messages.
Cisco ESA Initial Configuration

To perform the initial Cisco ESA configuration, complete the following steps:

**Step 1.** Log in to the Cisco ESA. The default username is admin, and the default password is ironport.

**Step 2.** Use the `systemsetup` command in the command-line interface (CLI) of the Cisco ESA to initiate the System Setup Wizard, as shown in Example 18-1.

---

**Example 18-1  Initial Setup with the systemsetup Command**

IronPort> systemsetup
WARNING: The system setup wizard will completely delete any existing 'listeners' and all associated settings including the 'Host Access Table' - mail operations may be interrupted.
Are you sure you wish to continue? [Y] > Y

You are now going to configure how the IronPort C60 accepts mail by creating a "Listener".

Please create a name for this listener (Ex: "InboundMail"):[]>

InboundMail

Please choose an IP interface for this Listener.
1. Management (192.168.42.42/24: mail3.example.com)
2. PrivateNet (192.168.1.1/24: mail3.example.com)
3. PublicNet (192.168.2.1/24: mail3.example.com)
[1]> 3

Enter the domains or specific addresses you want to accept mail for.
Hostnames such as "example.com" are allowed.
Partial hostnames such as ".example.com" are allowed.
Usernames such as "postmaster@" are allowed.
Full email addresses such as "joe@example.com" or "joe@1.2.3.4" are allowed.
Separate multiple addresses with commas
[]> securemeinc.org

Would you like to configure SMTP routes for example.com? [Y] > Y
Enter the destination mail server which you want mail for example.com to be delivered.
Separate multiple entries with commas.
[]> exchange.securemeinc.org
Do you want to enable rate limiting for this listener? (Rate limiting defines the maximum number of recipients per hour you are willing to receive from a remote domain.) [Y] > y

Enter the maximum number of recipients per hour to accept from a remote domain.
[1] > 4500

Default Policy Parameters

Maximum Message Size: 100M
Maximum Number Of Connections From A Single IP: 1,000
Maximum Number Of Messages Per Connection: 1,000
Maximum Number Of Recipients Per Message: 1,000
Maximum Number Of Recipients Per Hour: 4,500
Maximum Recipients Per Hour SMTP Response:
452 Too many recipients received this hour
Use SenderBase for Flow Control: Yes
Virus Detection Enabled: Yes
Allow TLS Connections: No

Would you like to change the default host access policy? [N] > n

Listener InboundMail created.

Use the listenerconfig->EDIT command to customize the listener.
******

Do you want to configure the C60 to relay mail for internal hosts? [Y] > y

Please create a name for this listener (Ex: "OutboundMail"): [1] > OutboundMail

Please choose an IP interface for this Listener.
1. Management (192.168.42.42/24: mail3.example.com)
2. PrivateNet (192.168.1.1/24: mail3.example.com)
3. PublicNet (192.168.2.1/24: mail3.example.com)

[1] > 2

Please specify the systems allowed to relay email through the IronPort C60.

Hostnames such as "example.com" are allowed.
Partial hostnames such as ".example.com" are allowed.
IP addresses, IP address ranges, and partial IP addressed are allowed.
Separate multiple entries with commas.
[]>.securemeinc.org

Do you want to enable rate limiting for this listener? (Rate limiting defines the maximum number of recipients per hour you are willing to receive from a remote domain.)
[N]> n

Default Policy Parameters
=================================
Maximum Message Size: 100M
Maximum Number Of Connections From A Single IP: 600
Maximum Number Of Messages Per Connection: 10,000
Maximum Number Of Recipients Per Message: 100,000
Maximum Number Of Recipients Per Hour: Disabled
Use SenderBase for Flow Control: No
Virus Detection Enabled: Yes
Allow TLS Connections: No
Would you like to change the default host access policy? [N]> n

Listener OutboundMail created.
Defaults have been set for a Private listener.
Use the listenerconfig->EDIT command to customize the listener.
*****

Congratulations! System setup is complete. For advanced configuration, please refer to the User Guide.

In Example 18-1, the inside (private) and outside (public) listeners are configured. The domain name of securemeinc.org is used in this example.

To verify the configuration, you can use the mailconfig command to send a test e-mail containing the system configuration data that was entered in the System Setup Wizard, as shown in Example 18-2.

**Example 18-2  Verifying the Configuration with the mailconfig Command**

```
mail3.securemeinc.org> mailconfig

Please enter the email address to which you want to send the configuration file. Separate multiple addresses with commas.
[]> admin@securemeinc.org

The configuration file has been sent to admin@securemeinc.org.

mail3.securemeinc.org>
```

In Example 18-2, the e-mail is sent to the administrator (admin@securemeinc.org).
Mitigation Technology for Web-Based Threats

For any organization to be able to protect its environment against web-based security threats, the security administrators need to deploy tools and mitigation technologies that go far beyond traditional blocking of known bad websites. Nowadays, you can download malware through compromised legitimate websites, including social media sites, advertisements in news and corporate sites, gaming sites, and many more. Cisco has developed several tools and mechanisms to help their customers combat these threats. The core solutions for mitigating web-based threats are the Cisco Cloud Web Security (CWS) offering and the integration of advanced malware protection (AMP) to the Cisco Web Security Appliance (WSA). Both solutions enable malware detection and blocking, continuous monitoring, and retrospective alerting. The following sections cover the Cisco CWS and Cisco WSA in detail.

Cisco CWS

Cisco CWS is a cloud-based security service from Cisco that provides worldwide threat intelligence, advanced threat defense capabilities, and roaming user protection. The Cisco CWS service uses web proxies in Cisco’s cloud environment that scan traffic for malware and policy enforcement. Cisco customers can connect to the Cisco CWS service directly by using a proxy autoconfiguration (PAC) file in the user endpoint or through connectors integrated into the following Cisco products:

- Cisco ISR G2 routers
- Cisco ASA
- Cisco WSA
- Cisco AnyConnect Secure Mobility Client

Organizations using the transparent proxy functionality through a connector can get the most out of their existing infrastructure. In addition, the scanning is offloaded from the hardware appliances to the cloud, reducing the impact to hardware utilization and reducing network latency. Figure 18-3 illustrates how the transparent proxy functionality through a connector works.

In Figure 18-3, the Cisco ASA is enabled with the Cisco CWS connector at a branch office. The following steps explain how Cisco CWS protects the corporate users at the branch office:

1. An internal user makes an HTTP request to an external website (securemeinc.org).
2. The Cisco ASA forwards the request to Cisco CWS global cloud infrastructure.
3. It notices that securemeinc.org had some web content (ads) that were redirecting the user to a known malicious site.
4. Cisco CWS blocks the request to the malicious site.
Cisco WSA

The Cisco WSA uses cloud-based intelligence from Cisco to help protect the organization before, during, and after an attack. This "lifecycle" is what is referred to as the *attack continuum*. The cloud-based intelligence includes web (URL) reputation and zero-day threat intelligence from Cisco's security intelligence and research group named Talos. This threat intelligence helps security professionals to stop threats before they enter the corporate network, while also enabling file reputation and file sandboxing to identify threats during an attack. Retrospective attack analysis allows security administrators to investigate and provide protection after an attack when advanced malware might have evaded other layers of defense.

The Cisco WSA can be deployed in explicit proxy mode or as a transparent proxy using the *Web Cache Communication Protocol (WCCP)*. WCCP is a protocol originally developed by Cisco, but several other vendors have integrated it in their products to allow clustering and transparent proxy deployments on networks using Cisco infrastructure devices (routers, switches, firewalls, and so on).

Figure 18-4 illustrates a Cisco WSA deployed as an explicit proxy.
Figure 18-4  *Explicit Proxy Configuration*

The following are the steps illustrated in Figure 18-4:

1. An internal user makes an HTTP request to an external website. The client browser is configured to send the request to the Cisco WSA.
2. The Cisco WSA connects to the website on behalf of the internal user.
3. The firewall (Cisco ASA) is configured to only allow outbound web traffic from the Cisco WSA, and it forwards the traffic to the web server.

Figure 18-5 shows a Cisco WSA deployed as a transparent proxy.

Figure 18-5  *Transparent Proxy Configuration*

The following are the steps illustrated in Figure 18-5:

1. An internal user makes an HTTP request to an external website.
2. The internal router (R1) redirects the web request to the Cisco WSA using WCCP.
3. The Cisco WSA connects to the website on behalf of the internal user.
4. Also in this example, the firewall (Cisco ASA) is configured to only allow outbound web traffic from the WSA. The web traffic is sent to the Internet web server.

Figure 18-6 demonstrates how the WCCS registration works. The Cisco WSA is the WCCP client, and the Cisco router is the WCCP server.
During the WCCP registration process, the WCCP client sends a registration announcement ("Here I am") every 10 seconds. The WCCP server (the Cisco router in this example) accepts the registration request and acknowledges it with an "I See You" WCCP message. The WCCP server waits 30 seconds before it declares the client as "inactive" (engine failed). WCCP can be used in large-scale environments. Figure 18-7 shows a cluster of Cisco WSAs, where internal Layer 3 switches redirect web traffic to the cluster.

The Cisco WSA comes in different models. The following are the different Cisco WSA models:
Cisco WSA S680
- It is a high-performance WSA designed for large organizations with 6000 to 12,000 users.
- A 2 rack-unit (RU) appliance with 16 (2 octa core) CPUs, 32 GB of memory, and 4.8 TB of disk space.

Cisco WSA S670
- A high-performance WSA designed for large organizations with 6000 to 12,000 users.
- A 2 RU appliance with 8 (2 octa core) CPUs, 8 GB of memory, and 2.7 TB of disk space.

Cisco WSA S380
- Designed for medium-size organizations with 1500 to 6000 users.
- A 2 RU appliance with 6 (1 hexa core) CPUs, 16 GB of memory, and 2.4 TB of disk space.

Cisco WSA S370
- Designed for medium-size organizations with 1500 to 6000 users.
- A 2 RU appliance with 4 (1 quad core) CPUs, 4 GB of memory, and 1.8 TB of disk space.

Cisco WSA S170
- Designed for small- to medium-size organizations with up to 1500 users.
- A 1 RU appliance with 2 (1 dual core) CPUs, 4 GB of memory, and 500 GB of disk space.

The Cisco WSA runs Cisco AsyncOS operating system. The Cisco AsyncOS supports numerous features that will help mitigate web-based threats. The following are examples of these features:

- **Real-time antimalware adaptive scanning**: The Cisco WSA can be configured to dynamically select an antimalware scanning engine based on URL reputation, content type, and scanner effectiveness. Adaptive scanning is a feature designed to increase the “catch rate” of malware that is embedded in images, JavaScript, text, and Adobe Flash files. Adaptive scanning is an additional layer of security on top of Cisco WSA Web Reputation Filters that include support for Sophos, Webroot, and McAfee.

- **Layer 4 traffic monitor**: Used to detect and block spyware. It dynamically adds IP addresses of known malware domains to a database of sites to block.

- **Third-party DLP integration**: Redirects all outbound traffic to a third-party DLP appliance, allowing deep content inspection for regulatory compliance and data exfiltration protection. It enables an administrator to inspect web content by title, metadata, and size and to even prevent users from storing files to cloud services, such as Dropbox, Google Drive, and others.

- **File reputation**: Using threat information from Cisco Talos, this file reputation threat intelligence is updated every 3 to 5 minutes.
Chapter 18: Mitigation Technologies for E-mail-Based and Web-Based Threats

- **File sandboxing**: If malware is detected, the Cisco AMP capabilities can put files in a sandbox to inspect its behavior, combining the inspection with machine-learning analysis to determine the threat level. Cisco Cognitive Threat Analytics (CTA) uses machine-learning algorithms to adapt over time.

- **File retrospection**: After a malicious attempt or malware is detected, the Cisco WSA continues to cross-examine files over an extended period of time.

- **Application visibility and control**: Allows the Cisco ASA to inspect and even block applications that are not allowed by the corporate security policy. For example, an administrator can allow users to use social media sites like Facebook but block micro-applications such as Facebook games.

**Cisco Content Security Management Appliance**

Cisco Security Management Appliance (SMA) is a Cisco product that centralizes the management and reporting for one or more Cisco ESAs and Cisco WSAs. Cisco SMA has consistent enforcement of policy, and enhances threat protection. Figure 18-8 shows a Cisco SMA that is controlling Cisco ESA and Cisco WSAs in different geographic locations (New York, Raleigh, Chicago, and Boston).

![Cisco SMA Centralized Deployment](image)

**Figure 18-8** *Cisco SMA Centralized Deployment*
The Cisco SMA comes in different models. These models are physical appliances or the Cisco Content Security Management Virtual Appliance (SMA V). The following are the different Cisco SMA models:

- **Cisco SMA M680**: Designed for large organizations with over 10,000 users
- **Cisco SMA M600v**: Designed for large enterprises or service providers
- **Cisco SMA M380**: Designed for organizations with 1000 to 10,000 users
- **Cisco SMA M300v**: Designed for organizations with 1000 to 5000 users
- **Cisco SMA M170**: Designed for small business or branch offices with up to 1000 users
- **Cisco SMAV M100v**: Designed for small business or branch offices with up to 1000 users

**NOTE** Cisco also has a Cisco SMA V M000v that is used for evaluations only.
Exam Preparation Tasks

Review All the Key Topics

Review the most important topics from this chapter, denoted with a Key Topic icon. Table 18-2 lists these key topics.

<table>
<thead>
<tr>
<th>Key Topic Element</th>
<th>Description</th>
<th>Page Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Section</td>
<td>E-mail-Based Threats</td>
<td>479</td>
</tr>
<tr>
<td>Section</td>
<td>Cisco Cloud E-mail Security</td>
<td>479</td>
</tr>
<tr>
<td>Section</td>
<td>Cisco E-mail Security Appliance</td>
<td>480</td>
</tr>
<tr>
<td>Section</td>
<td>Mitigation Technology for Web-Based Threats</td>
<td>486</td>
</tr>
<tr>
<td>Section</td>
<td>Cisco CWS</td>
<td>486</td>
</tr>
<tr>
<td>Section</td>
<td>Cisco WSA</td>
<td>487</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. There are no applicable tables in this specific chapter.

Define Key Terms

Define the following key terms from this chapter, and check your answers in the glossary:
- antispam filters
- network antivirus
- advanced malware protection (AMP)
- file sandboxing
- file retrospection

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 18-3 with a piece of paper, read the descriptions on the right side, and see whether you remember the commands.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>systemsetup</td>
<td>Launch the System Setup Wizard to initially configure the Cisco ESA.</td>
</tr>
<tr>
<td>mailconfig</td>
<td>Verify the Cisco ESA configuration by sending a test e-mail that contains the system configuration data that was entered in the system setup wizard.</td>
</tr>
</tbody>
</table>
Index

Numbers

3DES (Triple Digital Encryption Standard), 94, 124
802.1AB, 252
802.1Q, 238-239
802.1w, 245-246

AAA (authentication, authorization, and accounting)

ACS (Access Control Server)
  ACS configuration, 51-60
  benefits of, 38
  ISE (Identity Services Engine), 39
  RADIUS (Remote Authentication Dial-In User Service), 39-40
  router configuration, 41-50
  supported platforms, 38
  TACACS+ (Terminal Access Control Access Control Server), 39-40, 45
  troubleshooting, 60-66
Cisco Secure ACS Solution Engine, 283
components, 282
IPv4/IPv6, 332
method lists, 285-286, 292-296
overview, 35, 75, 106, 279-286, 359
router access authentication, 284-285
self-contained AAA, 283
troubleshooting, 296-301
verifying, 43-45
VPN user authentication, 283-284
aaa authentication command, 318
aaa authentication login command, 42, 68
aaa authentication login default local command, 318
aaa authorization exec command, 42, 68
aaa new-model command, 41, 45, 68, 292, 303, 318
acceptable use policy (AUP), 11
access-class command, 374
access control. See also ACS (Access Control Server)
access rules
  ASA (Adaptive Security Appliance), 447-449
  firewalls, 371
ACE (access control entry), 345, 374
ACLs (access control lists), 136, 270, 360
  ACL logging, 345
  firewalls, 374
  IPv6 security, 337
  packet filtering ACLs, 423
Cisco ESA (E-mail Security Appliance), 481
access control entry (ACE), 345, 374
access control lists. See ACLs
Access Control Server. See ACS (Access Control Server)
access-list 2 permit command, 407
access rules
ASA (Adaptive Security Appliance), 447-449
firewalls, 371
accounting. See AAA (authentication, authorization, and accounting)
ACE (access control entry), 345, 374
ACLs (access control lists), 136, 270, 360
ACL logging, 345
firewalls, 374
IPv6 security, 337
packet filtering ACLs, 423
ACS (Access Control Server)
ACS configuration, 51-52
authorization policies, 56-57
authorization profiles, 58-60
identity groups, 56
network device groups, 53-54
user groups, 54
benefits of, 38
ISE (Identity Services Engine), 39
overview, 14, 35, 38
RADIUS (Remote Authentication Dial-In User Service), 39-40
router configuration
AAA verification, 43-45
CCP (Cisco Configuration Professional), 45-50
CLI (command line interface), 41-43
overview, 41
TACACS+, 45
supported platforms, 38
TACACS+ (Terminal Access Control
Access Control Server), 39-40, 45
troubleshooting
basic connectivity, 60
debug command, 62-66
ping command, 60
test command, 60-62
activating Pearson Cert Practice Test (PCPT) software, 506
Active Directory (AD), 76
Adaptive Security Appliance. See ASA (Adaptive Security Appliance)
Adaptive Security Device Manager. See ADSM (Adaptive Security Device Manager)
Address Resolution Protocol. See ARP (Address Resolution Protocol)
addresses
ARP (Address Resolution Protocol), 325
DAI (Dynamic ARP Inspection), 254-256
overview, 233
poisoning, 14, 271
spoofing, 271
bogon addresses, 336
IPv6, 325
all-nodes multicast addresses, 328
all-routers multicast addresses, 328
anycast addresses, 328
configuring, 326-327
conversion between decimal, binary, and hexadecimal, 326
length, 325
link-local addresses, 327
loopback addresses, 327
addresses

solicited-node multicast addresses, 328
unicast addresses, 328
Network Address Translation. See NAT (Network Address Translation)
administrative controls, 11
ADSM (Adaptive Security Device Manager), 107-108, 422
Advanced Encryption Standard (AES), 94, 124
advanced malware protection (AMP), 419, 473, 477, 481, 499
AMP for Endpoints, 31, 499-500
AES (Advanced Encryption Standard), 94, 124
agents (SNMP), 310
Aggregation Services Routers (ASR), 75
AH (Authentication Header), 97
alarms
monitoring, 471
security intelligence, 471-472
alerts, 466
monitoring, 471
security intelligence, 471-472
algorithms, 91. See also cryptography
asymmetric algorithms, 93-94
Cipher Block Chaining Data Encryption Standard (DES-56) algorithm, 311
encryption algorithms, 124
hash algorithms, 124
RSA algorithm, 99-100
symmetric algorithms, 93
all-nodes multicast addresses, 328
all-routers multicast addresses, 328
AMBER classification level (TLP), 9
AMP (advanced malware protection), 419, 473, 477, 481, 499
AMP for Endpoints, 31, 499-500
amplification attacks, 28
annotations (STP), 242-245
anomaly-based IPS/IDS, 464-465
antimalware solutions, 497-498
antimalware adaptive scanning, 490
antivirus solutions, 29, 497-498
Cisco ESA (E-mail Security Appliance), 481
antiphishing defenses, 29
antireplay protection
IPsec, 122
VPNs (virtual private networks), 90
antispam, 481
antivirus solutions, 29, 497-498
anycast addresses, 328
AnyConnect Secure Mobility Client. See Cisco AnyConnect Secure Mobility Client
application inspection, 417
application inspection firewalls, 364-365
application layer attacks, 333
application layer gateways, 363
AR (attack relevancy), 468
architecture
BYOD (bring your own device), 74
security guidelines, 16-17
topologies
CAN (Campus Area Network), 17
Cloud/WAN (Wide Area Network), 18
Data Center network, 18-19
SOHO (small office/home office), 18
virtual environments, 20-21
ARP (Address Resolution Protocol), 325
DAI (Dynamic ARP Inspection), 254-256
overview, 233
poisoning, 14, 271
spoofing, 271
ASA (Adaptive Security Appliance)
access rules, 447-449
ASDM GUI, 433-435
basic routing, 444-445
default traffic flow, 420-422
DHCP service, 443-444
digital certificate installation, 107
  default certificate, 108
  identity certificates, 111-114
  root certificates, 109-114
features/services, 417-419
ICMP echo requests, 433
initial access, 422
initial boot, 425-431
initial setup script, 432-433
interface configuration, 435-443
IPsec site-to-site VPN implementation, 179-192
  commands sent to Cisco ASA, 184-189
  connection profiles, 189-191
IKE policy, 191
IKEv1 policies, 191
IKEv2 settings, 192
IPsec proposals (transform sets), 192
local/remote networks, 181-182
NAT Exempt policy, 183
peer device identification, 180
security options, 182
traffic to protect, 180-181
IPsec site-to-site VPN troubleshooting, 193-198
d debug command, 198
show crypto ipsec sa command, 195-196
show crypto isakmp stats command, 193
show isakmp sa detail command, 196-197
show isakmp stats command, 193-195
show vpn-sessiondb command, 197
models, 416
MPF (Modular Policy Framework), 424
NAT (Network Address Translation), 445-447
No Telnet policy, 453
overview, 75, 413
packet filtering, 422-423
Packet Tracer, 449-453
PAT (Port Address Translation), 445-447
policy application, 425
security levels, 419-420
SSL clientless VPN configuration
  CLI (command line interface), 214-215
  connection profile access, 211
digital certificates, 211
login, 215-216
SSL VPN Wizard, 209-210
user authentication, 211-214
VPN statistics, 217
tools to manage, 422
ASA Security Device Manager (ASDM), 433-435
ASA with FirePOWER services, 473
ASDM (ASA Security Device Manager), 433-435
ASR (Aggregation Services Routers), 75
ASR (attack severity rating), 467, 470
assets
classifying, 8-10
defined, 7-8
asymmetric algorithms, 93-94
asymmetric key cryptography, 99
atomic micro-engine, 470
attack relevancy (AR), 468
attack severity rating (ASR), 467, 470
attacks
AR (attack relevancy), 468
attack vectors, 14
back doors, 13
botnets, 15
brute-force attacks, 15
code execution attacks, 13
cover covert channel, 15
data loss and exfiltration methods, 31-32
DDoS (distributed denial-of-service) attacks, 16, 27-28
DoS (denial-of-service) attacks, 16, 27-28
e-mail-based threats
Cisco cloud e-mail security, 479
Cisco ESA (E-mail Security Appliance), 480-485
Cisco hybrid e-mail security, 480
malware attachments, 479
phishing, 479
spam, 479
spear phishing, 479
IPv4/IPv6 threats, 333-336
malware identification tools, 30-31
Cisco AMP (Advanced Malware Protection), 31
IPS events, 31
NetFlow, 30
NGIPS (next-generation intrusion prevention system), 31
packet captures, 30
Snort, 30
man-in-the-middle attacks, 14-15
motivation behind, 27
pharming, 13
phishing, 13
potential attackers, 12
privilege escalation, 13
reconnaissance, 13
social engineering, 13, 28-30
defenses against, 29-30
malvertising, 29
phishing, 29
phone scams, 29
trust exploitation, 15
web-based threats
Cisco CWS (Cloud Web Security), 486
Cisco SMA (Security Management Appliance), 491-492
Cisco WSA (Web Security Appliance), 487-491
auditing, 17
AUP (acceptable use policy), 11
authentication, 125. See also AAA (authentication, authorization, and accounting)
CAs (certificate authorities), 104
defined, 96
e-mail, 481
IPsec site-to-site VPNs, 122, 153
peer authentication, 126
routing update authentication
on OSPF, 348-350
on RIP, 350-352
SNMP (Simple Network Management Protocol), 312
SSL clientless VPN configuration, 211-214
two-factor authentication, 29
VPNs (virtual private networks), 90
Authentication Header (AH), 97
authentication keyword, 349
authNoPriv security level, 311
authorization. See also AAA
(authentication, authorization, and accounting)
authorization policies (ACS), 56-57
authorization profiles (ACS), 58-60
authPriv security level, 311
auto secure command, 266
autoconfiguration, 335
availability, 6
AxCrypt, 501

B
back doors, 13, 497
Basic Firewall Wizard, 386-388
Basic NAT Wizard, 405-407
BCP (best common practices), 74
best practices
BCP (best common practices), 74
IPS/IDS, 472
IPv4 security, 332-333
IPv6 security, 332-336
Layer 2 security, 246-247
management plane security, 278-280
NFP (Network Foundation Protection)
control plane security, 268-269
data plane security, 271
management plane security, 267-268
BGP routing update authentication, 351-352
binary, converting to decimal/hexadecimal, 326
BitLocker, 501
block ciphers, 92
blocking connections, 466
blue rollover cable, 278
bogon addresses, 336
botnets, 15, 419
BPDU (bridge protocol data units), 242
BPDU Guard, 248-249
bridge protocol data units (BPDU), 242
bring your own device. See BYOD
(bring your own device)
brute-force attacks, 15
buffer, 288
BYOD (bring your own device)
architecture framework, 74
as attack vector, 14
business reasons for, 73
MDM (mobile device management)
cloud-based deployment, 78-79
on-premise deployment, 77-78
overview, 76
solution components, 74-76

C
C3PL (Cisco Common Classification Policy Language), 381
CA (certificate authority), 76, 96, 208
authenticating and enrolling with, 104
explained, 100-101
cables, blue rollover cable, 278

cache, neighbor cache resource starvation, 334

Call Manager Express (CME), 388

CAM (content-addressable memory), 250, 271, 333

CAM table overflow attack, 250

Campus Area Network (CAN), 17

CAN (Campus Area Network), 17

CBAC (context-based access control), 270

CCNA Security
BPDU Guard, 248-249
port security, 250-251
Root Guard, 249

CCP (Cisco Configuration Professional), 41, 129
router configuration with ACS (Access Control Server), 45-50

ZBF (Zone-Based Firewall) configuration, 385-391

CLI commands created by CCP, 391-399

CME (Call Manager Express), 388-389

DNS servers, 390
interfaces, 387-388
security level, 388-389
verifying, 399-400

CDP (Cisco Discovery Protocol)
disabling, 252
overview, 251-252

CEF (Cisco Express Forwarding)-Exception traffic, 269

CEF (Cisco Express Forwarding) table, 344

certificate authority. See CA (certificate authority)
certificate revocation list (CRL), 106, 208
certificates. See digital certificates
Certification Path Answer (CPA), 336
Certification Path Solicitation (CPS), 336
change management, 29
CIFS (Common Internet File System), 215
Cipher Block Chaining Data Encryption Standard (DES-56) algorithm, 311
cipher digit stream, 92
ciphers, 91
block ciphers, 92
defined, 91
polyalphabetic, 91
stream ciphers, 92
substitution, 91
symmetric ciphers, 93
transposition, 91
circumventing IPS/IDS, 468-469
Cisco Access Control Server. See ACS (Access Control Server)
Cisco AMP (Advanced Malware Protection) for Endpoints, 31, 499-500
Cisco AnyConnect Secure Mobility Client
Cisco AnyConnect Secure Mobility Client Wizard, 218
authentication method, 220-221
connection profiles, 218-219
DNS entries, 221-222
exemptions from NAT, 222-223
IP address pool information, 220-221
protocols to support, 219
software packages to deploy, 220
class maps

Summary screen, 223-224
Welcome screen, 218
overview, 75
troubleshooting
   initial connectivity issues, 228-229
   traffic-specific issues, 230
Cisco ASR (Aggregation Services Routers), 75
Cisco cloud e-mail security, 479
Cisco Common Classification Policy Language (C3PL), 381
Cisco Configuration Professional. See CCP (Cisco Configuration Professional)
Cisco CWS (Cloud Web Security), 75, 486
Cisco Discovery Protocol. See CDP (Cisco Discovery Protocol)
Cisco E-mail Security Appliance. See ESA (E-mail Security Appliance)
Cisco Express Forwarding (CEF)-Exception traffic, 269
Cisco Express Forwarding (CEF) table, 344
Cisco FirePOWER, 31
Cisco FireSIGHT Management Center, 31
Cisco hybrid e-mail security, 480
Cisco IDS. See IDS (intrusion detection systems)
Cisco ISE (Identity Services Engine), 75
Cisco IOS devices
   IPsec site-to-site VPN implementation, 155-164
      crypto policy, 162-164
      digital certificates, 158-159
   NTP configuration, 156
   NTP status verification, 157
   Site-to-Site VPN Wizard, 159-162
   IPSec site-to-site VPN troubleshooting, 164-178
      debug command, 165-166
      IKEv1 Phase 1 policy, 170-174
      IKEv1 Phase 2 policy, 174-178
      ping command, 165-170
   verification of IPsec configuration, 164-168
file protection
   configuring, 315-316
   overview, 289-290
management plane security. See management plane security
Zone-Based Firewalls. See ZBFs (Zone-Based Firewalls)
Cisco IPS. See IPS (intrusion prevention systems)
Cisco ISR (Integrated Services Routers), 75
Cisco Learning Network, 507
Cisco NGIPS (Next-Generation IPS), 472-473
Cisco Secure ACS Solution Engine, 283
Cisco Security Manager (CSM), 266, 471
Cisco SenderBase, 481
Cisco SIO (Security Intelligence Operations), 472, 481
Cisco SMA (Security Management Appliance), 491-492
Cisco Sourcefire, 498
Cisco WSA (Web Security Appliance), 477, 487-491
ClamAV, 498
class maps, 381
class-map type inspect match-any command, 410
class type inspect command, 410
classic IOS, 289

classifying
assets, 8-10
countermeasures, 10-11
information classification policies, 29
vulnerabilities, 10

CLI (command-line interface), 129. See also individual commands
crypto policy implementation, 162-164
IPsec configuration, 137-139
router configuration for ACS (Access Control Server), 41-43
SSL clientless VPN configuration, 214-215
ZBFs (Zone-Based Firewalls)
  commands created by CCP, 391-399
  verifying, 400-404
client. See Cisco AnyConnect Secure Mobility Client
cloud-based MDM (mobile device management) deployment, 78-79

Cloud/WAN (Wide Area Network), 18
Cloud Web Security (CWS), 75, 486
CME (Call Manager Express), 388

code execution attacks, 13
collision resistance, 94
command-line interface. See CLI (command-line interface)
Common Internet File System (CIFS), 215
Common Vulnerabilities and Exposures (CVE), 10
community strings, 311

confidentiality, 6
IPsec site-to-site VPNs, 122, 152
VPNs (virtual private networks), 89-90

configuration
ACS (Access Control Server), 51-52
  authorization policies, 56-57
  authorization profiles, 58-60
  identity groups, 56
  network device groups, 53-54
  user groups, 54
ASA (Adaptive Security Appliance)
  access rules, 447-449
  ASDM GUI, 433-435
  basic routing, 444-445
  DHCP service, 443-444
  ICMP echo requests, 433
  initial boot, 425-431
  initial setup script, 432-433
  interfaces, 435-443
  NAT (Network Address Translation), 445-447
  No Telnet policy, 453
  Packet Tracer, 449-453
  PAT (Port Address Translation), 445-447
BPDU Guard, 248
Cisco AnyConnect Secure Mobility Client, 217
  connection profiles, 225-226
  full-tunnel SSL VPN configuration, 218-225
  groups, 225-226
  split tunneling, 227-228
  troubleshooting, 228-230
  tunnel groups, 226
  types of SSL VPNs, 218
Cisco ESA (E-mail Security Appliance), 483-485
CoPP (control plane policing), 346-347
DAI (Dynamic ARP Inspection), 256
DHCP (Dynamic Host Configuration Protocol) snooping, 254
IPsec
  CLI (command-line interface)
  equivalent comments, 137-139
  completing and verifying, 139-145
  planning, 129
Quick Setup Wizard, 129-130
Step by Step VPN Wizard, 130-137
tools, 129
IPv6
  addresses, 326-327
  routing, 330-331
MD5 authentication
  on BGP, 352
  on EIGRP, 350
  on OSPF, 349
  on RIPv2, 351
NAT (Network Address Translation), 404-408
NTP (Network Time Protocol), 313-315
NTP services, 156
port security, 250-251
PortFast, 245-246
recovery of err-disabled ports, 249
router configuration with ACS (Access Control Server)
  AAA verification, 43-45
  CCP (Cisco Configuration Professional), 45-50
  CLI (command line interface), 41-43
overview, 41
TACACS+, 45
RST (Rapid Spanning Tree), 245-246
SCP (Secure Copy Protocol), 315
secure bootset, 315-316
SNMP (Simple Network Management Protocol), 312-313
SSL clientless VPN
  CLI (command line interface), 214-215
  connection profile access, 211
digital certificates, 211
  login, 215-216
SSL VPN Wizard, 209-210
  user authentication, 211-214
  VPN statistics, 217
Syslog, 308-310
trunk ports, 238-239
ZBFs (Zone-Based Firewalls)
  verifying from command line, 400-404
  verifying with CCP, 385-400
connection profiles
Cisco AnyConnect Secure Mobility Client, 225-226
IPsec site-to-site VPNs, 189-191
SSL clientless VPN configuration, 211
content-addressable memory (CAM), 250, 271, 333
context-based access control (CBAC), 270
control plane policing. See CoPP (control plane policing)
control plane protection (CPPr), 269, 348
control plane security

CoPP (control plane policing), 346-347
  configuration, 346-347
  verification, 347

CPPr (control plane protection), 269, 348

impact of control plane traffic on CPU, minimizing, 344-345

overview, 264, 268, 344

routting update authentication
  on BGP, 351-352
  on EIGRP, 349-350
  on OSPF, 348-349
  on RIP, 350-351

security best practices, 268-269

threat control and mitigation strategy, 265

conversion between decimal, binary, and hexadecimal, 326

coordinated universal time (UTC), 156

CoPP (control plane policing), 269, 346-347
  configuration, 346-347
  verification, 347

Core module (BYOD), 78

cost-benefit analysis of security, 7

countermeasures
  classifying, 10-11
  defined, 7-8

covet channel, 15

CPA (Certification Path Answer), 336

CPPr (control plane protection), 269, 348

CPS (Certification Path Solicitation), 336

credit cards, 32

CRL (certificate revocation list), 106, 208

cross-certifying CAs (certificate authorities), 107

crypto ACL, 136

crypto ca authenticate command, 113, 117

crypto ca enroll command, 113, 117

crypto ikev1 policy command, 200

crypto ikev2 policy command, 200

crypto ipsec ikev1 transform-set command, 200

crypto ipsec ikev2 transform-set command, 200

crypto ipsec security-association lifetime command, 155

crypto ipsec transform-set command, 138, 147, 163, 200

crypto isakmp policy command, 137, 147, 154, 162, 200

crypto key generate rsa command, 117, 158, 318

Crypto Locker, 498

crypto map command, 139, 147, 163-164, 175, 200

crypto maps, 136

crypto pki authenticate command, 158

crypto pki enroll command, 158

crypto policy, 162-164

cryptography

  algorithms, 91

    asymmetric algorithms, 93-94

    Cipher Block Chaining Data Encryption Standard (DES-56) algorithm, 311

    encryption algorithms, 124

    hash algorithms, 124

    RSA algorithm, 99-100

    symmetric algorithms, 93
ciphers, 91
  block ciphers, 92
  defined, 91
  polyalphabetic, 91
  stream ciphers, 92
  substitution, 91
  symmetric ciphers, 93
  transposition, 91
digital signatures, 95-96
Hashed Message Authentication Code (HMAC), 95
hashes, 94-95
IPsec. See IPsec
key management, 92, 96-97
  keyspace, 96
  next-generation encryption protocols, 97
SSL (Secure Sockets Layer), 98
CryptoWall, 498
CSM (Cisco Security Manager), 266, 471
custom privilege levels (RBAC), 287, 301-303
customer needs for IPsec site-to-site VPNs, 152-153
CVE (Common Vulnerabilities and Exposures), 10
CWS (Cloud Web Security), 75, 486

D

DAI (Dynamic ARP Inspection), 14, 253-256, 271, 333
Data Center network, 18-19
data centers, 77-78
data integrity, 90, 122, 152
data location, 3
data loss and exfiltration methods, 31-32
data loss prevention (DLP), 76, 477, 480-481
data plane (NFP). See also IPv6
  additional protection mechanisms, 271
  defined, 264
  explained, 270
  security best practices, 271
  threat control and mitigation strategy, 266
DDoS (distributed denial-of-service) attacks, 16, 27-28, 335
debit cards, 32
debug aaa accounting command, 296
debug aaa authentication command, 296-297
debug aaa authorization command, 296-297
debug command, 62-66, 165-166, 198
debug crypto condition peer command, 201
debug crypto ikev1 ikev2 command, 198
debug crypto ikev2 platform 2 command, 198
debug crypto ikev2 protocol 2 command, 198
debug crypto ipsec command, 198, 201
debug crypto isakmp command, 201
debug webvpn anyconnect command, 229
debug webvpn svc command, 228-229
decimal, converting to binary/hexadecimal, 326
default traffic flow (ASA), 420-422
defense-in-depth approach, 16, 360-361
demilitarized zone (DMZ), 15, 359, 369, 420
denial-of-service (DoS) attacks, 6, 16, 27-28, 267, 332-333

deny ipv6 any command, 337

deployment

firewalls

access rules, 371
ACLs (access control lists), 374
design guidelines, 370-372
packet-filtering access rule structure, 372
rule implementation consistency, 373-374
technologies, 370

MDM (mobile device management)
cloud-based deployment, 78-79
on-premise deployment, 77-78

NAT (Network Address Translation), 369-370

DES (Digital Encryption Standard), 124
design of firewalls, 370-372
designated ports, 245
device groups (ACS), 53-54
device hardening, 332
DH (Diffie-Hellman) key exchange protocol, 94, 97, 124-126

DHCP (Dynamic Host Configuration Protocol), 271, 324, 328, 418

ASA (Adaptive Security Appliance) configuration, 443-444
DHCPv6, 335
snooping, 253-254
differentiated services code point (DSCP), 424

Diffie-Hellman (DH) key exchange protocol, 94, 97, 124-126
digests, 94

digital certificates

identity certificates, 102
installing on ASA, 107
default certificate, 108
identity certificates, 111-114
root certificates, 109-114
obtaining, 158-159
revoked certificates, 105-106
root certificates, 101-102
SSL clientless VPN configuration, 211
uses for, 106
X.500 certificates, 103
X.509 certificates, 103-104

Digital Encryption Standard (DES), 124

Digital Signature Algorithm (DSA), 94
digital signatures, 95-96, 100, 122, 469

micro-engines, 470
severity levels, 471
digital subscriber line (DSL), 87
direct DoS (denial-of-service) attacks, 27

disabling CDP (Cisco Discovery Protocol), 252

Disk Utility, 501
disruptive motivations behind threats, 27
distributed denial-of-service (DDoS) attacks, 16, 27-28
distributed DoS (DDoS) attacks, 335

DKIM (DomainKeys Identified Mail), 481

DLP (data loss prevention), 76, 477, 480-481

DMVPN (Dynamic Multipoint VPN), 178

DMZ (demilitarized zone), 15, 359, 369, 420
DNS (Domain Name System), 215, 324, 359

do show ipv6 interface brief command, 326

do show vlan brief command, 237
document handling and destruction, 29
Domain Name System (DNS), 215, 324, 359
DomainKeys Identified Mail (DKIM), 481
DoS (denial-of-service) attacks, 6, 16, 27-28, 267, 332-333
downloaders, 497
downloading Pearson Cert Practice Test (PCPT) software, 506
drop action, 382
DSA (Digital Signature Algorithm), 94
DSCP (differentiated services code point), 424
DSL (digital subscriber line), 87
dual stacks, 335
duties, separation of, 16
Dynamic ARP Inspection (DAI), 14, 254-256, 271, 333
Dynamic Host Configuration Protocol. See DHCP (Dynamic Host Configuration Protocol)
Dynamic Multipoint VPN (DMVPN), 178
dynamic NAT (Network Address Translation), 369

E

eavesdropping, 333
ECC (Elliptic Curve Cryptography), 94, 97
Edit IPsec Site-to-Site Connection Profile dialog box, 191
egress, 382

EIGRP (Enhanced Interior Gateway Routing Protocol), 268, 349-350
ElGamal, 94
Elliptic Curve Cryptography (ECC), 94, 97

e-mail security
Cisco cloud e-mail security, 479
Cisco ESA (E-mail Security Appliance), 480-482
initial configuration, 483-485
models, 480
supported features, 481-482
Cisco hybrid e-mail security, 480
e-mail authentication, 481
e-mail encryption, 481, 500-501
malware attachments, 479
overview, 477
phishing, 479
spam, 479
spear phishing, 479

E-mail Security Appliance. See ESA (E-mail Security Appliance)
enable password, 286
enable view command, 304, 318
Encapsulating Security Payload (ESP), 97, 128, 153
encrypted management protocols, 279, 287-288

encryption, 469. See also cryptography
algorithms, 124
asymmetric algorithms, 93-94
e-mail, 481, 500-501
encrypted management protocols, 279, 287-288
endpoint data at rest, 501
next-generation encryption protocols, 97
SNMP (Simple Network Management Protocol), 312
symmetric algorithms, 93
**endpoint threat mitigation techniques**, 495
antivirus/antimalware solutions, 497-498
Cisco AMP (Advanced Malware Protection) for Endpoints, 31, 499-500
e-mail encryption, 500-501
encryption of endpoint data at rest, 501
HIPS (host intrusion prevention systems), 498
personal firewalls, 498-499
VPNs (virtual private networks), 501-502
Enhanced Interior Gateway Routing Protocol (EIGRP), 268
enrolling with CAs (certificate authorities), 104
erd disable recovery cause bpduguard command, 249
ESA (E-mail Security Appliance), 477, 480-482
initial configuration, 483-485
models, 480
supported features, 481-482
ESP (Encapsulating Security Payload), 97, 128, 153
evading IPS/IDS, 468-469
exam engine
installing, 505
practice exam mode, 508-509
study mode, 508
study plan, 507-509
exam engine, 508-509
practice configurations, 508
recalling the facts, 507-508
exfiltration, 31-32
exploits, 497
F
FIFO (first in, first out), 288
file reputation, 490
file retrospection, 491
files
file protection (Cisco IOS)
configuring, 315-316
overview, 289-290
file sandboxing, 491
logging
overview, 288-289
Syslog configuration, 308-310
syslog security levels, 289
FileVault, 501
filtering
botnet traffic filtering, 419
packet filtering
explained, 417
stateful packet filtering, 363-364
static packet filtering, 362
stateful filtering, 417
URL (uniform resource locator) filtering, 379
financial motivations behind threats, 27
FirePOWER, 31
FireSIGHT Management Center, 31, 473
Firewall Wizard, 386
firewalls
  access rules, 371
  ACLs (access control lists), 374
  ASA (Adaptive Security Appliance)
    access rules, 447-449
    ASDM GUI, 433-435
    basic routing, 444-445
    default traffic flow, 420-422
    DHCP service, 443-444
    features/services, 417-419
    ICMP echo requests, 433
    initial access, 422
    initial boot, 425-431
    initial setup script, 432-433
    interface configuration, 435-443
    models, 416
    MPF (Modular Policy Framework), 424
  NAT (Network Address Translation), 445-447
  No Telnet policy, 453
  overview, 413
  packet filtering ACLs, 423
  packet filtering on ASA, 422-423
  Packet Tracer, 449-453
  PAT (Port Address Translation), 445-447
  policy application, 425
  security levels, 419-420
  tools to manage, 422
benefits of, 359
common properties, 358-359
defense-in-depth approach, 360-361
design guidelines, 370-372
IOS firewall support, 270
limitations of, 359-360
methodologies, 361
  application inspection firewalls, 364-365
  application layer gateways, 363
  NGFW (next-generation firewalls), 365
  stateful packet filtering, 363-364
  static packet filtering, 362
  transparent firewalls, 365
NAT (Network Address Translation)
  deployment options, 369-370
  dynamic NAT, 369
  NAT with overload, 368
  overview, 366-367
  PAT (Port Address Translation), 368-369
  policy NAT, 370
  static NAT, 369
  terminology, 367-368
objectives of, 358-359
overview, 355, 358
packet-filtering access rule structure, 372
personal firewalls, 498-499
proxy firewalls, 363
rule implementation consistency, 373-374
standards, 370
ZBFs (Zone-Based Firewalls), 377
  C3PL (Cisco Common Classification Policy Language), 381
  class maps, 381
  components, 383-384
  configuring with CCP (Cisco Configuration Professional), 385-399
  features, 379
how they work, 379
NAT (Network Address Translation), 404-408
policy maps, 381-382
self zones, 380, 384-385
service policies, 382-384
traffic interaction between zones, 383
verifying from command line, 400-404
verifying with CCP (Cisco Configuration Professional), 399-400
zones, 380
first in, first out (FIFO), 288
FlexVPN, 178
FQDN (fully qualified domain name), 100
frame forwarding, 239
framework (NFP), 264
full-tunnel SSL VPN configuration, 218-225
fully qualified domain name (FQDN), 100

G
Galois/Counter Mode (GCM), 97
gateways, application layer, 363
GCM (Galois/Counter Mode), 97
Generate Mirror button, 139
generic routing encapsulation (GRE), 469
geopolitical motivations behind threats, 27
GET message, 310
global correlation, 468
GPG, 501

GRE (generic routing encapsulation), 469
GREEN classification level (TLP), 10
group-policy command, 200
groups
Cisco AnyConnect Secure Mobility Client, 225-226
identity groups (ACS), 56
network device groups (ACS), 53-54
user groups (ACS), 54

H
hackers, 12
hactivists, 12
hash algorithms, 124
Hashed Message Authentication Code (HMAC), 95, 122, 152, 311
hashes, 94-95
hexadecimal, converting to decimal/binary, 326
hierarchical PKI (public key infrastructure) topology, 107
high availability, 419
HIPS (host intrusion prevention systems), 498
HMAC (Hashed Message Authentication Code), 95, 122, 152, 311
hop-by-hop extension headers, 335
host ID, 325
host intrusion prevention systems (HIPS), 498
HTTP (Hypertext Transfer Protocol), 360
HTTPS (Hypertext Transfer Protocol Secure), 15, 279, 307-308, 332, 360
ICMP (Internet Control Message Protocol), 15, 153, 271, 325, 384
ASA (Adaptive Security Appliance), 433
echo requests, 433
ICMPv6, 335
unreachable messages, 345
identity certificates, 102, 111-114
identity groups (ACS), 56
Identity Services Engine (ISE), 14, 39, 75
IDS (intrusion detection systems).
See also IPS (intrusion prevention systems)
alarms/alerts, 471-472
best practices, 472
compared to IPS (intrusion protection systems), 460-462
evasion techniques, 468-469
identification of malicious traffic, 463
anomaly-based IPS/IDS, 464-465
policy-based IPS/IDS, 464-465
reputation-based IPS/IDS, 464-465
RR (risk rating), 467-468
sensor responses to detected attacks, 465-467
signature-based IPS/IDS, 464-465
overview, 30, 457
sensors
defined, 460
responses to detected attacks, 465-467
sensor platforms, 462
signatures, 469
micro-engines, 470
severity levels, 470-471
ture/false negatives, 463
ture/false positives, 463
IETF (Internet Engineering Task Force), 207
IKE (Internet Key Exchange), 97, 123
IKEv1, 191
explained, 123
IKEv1 Phase 1 planning, 154, 170-174
IKEv1 Phase 1 tunnel negotiation, 124-125
IKEv1 Phase 2 planning, 154-155
IKEv1 Phase 2 policy, 174-178
IKEv2, 123, 192
IPsec site-to-site VPNs, 191
IME (IPS Manager Express), 471
Immunet, 498
information classification, 29
ingress, 382
initial boot (ASA), 425-431
initial setup script (ASA), 432-433
inside global NAT (Network Address Translation), 367
inside local NAT (Network Address Translation), 367
inspect action, 382
inspect keyword, 424
installing Pearson Cert Practice Test engine, 505
Integrated Services Routers (ISR), 75
integrity, 6, 312
intellectual property (IP), 31
interdependence (NFP), 265
interfaces, 447
  configuring
    on ASA (Adaptive Security Appliance), 435-443
    as trunk ports, 238-239
IPv6, 328-329
Internet Control Message Protocol (ICMP), 15, 153, 271, 325, 384
Internet edge, 77
Internet Engineering Task Force (IETF), 207
Internet Key Exchange. See IKE (Internet Key Exchange)
Internet Security Association and Key Management Protocol (ISAKMP), 123
Internet service providers (ISPs), 11
inter-VLAN routing, 240
intrusion detection systems. See IDS (intrusion detection systems)
intrusion prevention systems. See IPS (intrusion prevention systems)
IOS devices. See Cisco IOS devices
IOS firewall support, 270
IP (intellectual property), 31
ip access-group command, 374
IP addresses, assigning with ASA (Adaptive Security Appliance), 443-444
ip arp inspection trust command, 259
ip arp inspection vlan 10 command, 256, 259
ip dhcp snooping command, 254, 259
ip dhcp snooping trust command, 259
ip dhcp snooping vlan 10 command, 259
ip ospf authentication-key command, 348
ip ospf message-digest-key command, 348
ip scp server enable command, 318
IP Source Guard, 271
IPS (intrusion prevention systems). See also IDS (intrusion detection systems)
alarms/alarms
  monitoring, 471
  security intelligence, 471-472
best practices, 472
Cisco NGIPS (Next-Generation IPS), 472-473
compared to IDS (intrusion detection systems), 460-462
evasion techniques, 468-469
identification of malicious traffic, 463
anomaly-based IPS/IDS, 464-465
policy-based IPS/IDS, 464-465
reputation-based IPS/IDS, 464-465
RR (risk rating), 467-468
sensor responses to detected attacks, 465-467
signature-based IPS/IDS, 464-465
overview, 7, 75, 227, 270, 359, 424, 457
sensors
  defined, 460
  responses to detected attacks, 465-467
  sensor platforms, 462
signatures, 469
  micro-engines, 470
  severity levels, 470-471
ture/false negatives, 463
ture/false positives, 463
IPS events, 31
IPSec (Internet security)

AH (Authentication Header), 97
compared to SSL (Secure Sockets Layer), 206
configuration
  CLI (command-line interface)
    equivalent comments, 137-139
  completing and verifying,
    139-145
  planning, 129
  Quick Setup Wizard, 129-130
  Step by Step VPN Wizard,
    130-137
  tools, 129
defined, 88, 97
ESP (Encapsulating Security Payload), 97
goals of, 122-123
IKE (Internet Key Exchange), 123-125
overview, 119
site-to-site VPNs
  alternatives to, 178
  customer needs, 152-153
  IKEv1 Phase 1 planning, 154
  IKEv1 Phase 2 planning,
    154-155
  implementing in Cisco ASA,
    179-192
  implementing in Cisco IOS
devices, 155-164
overview, 149
required protocols, 153
troubleshooting in Cisco ASA,
  193-198
troubleshooting in Cisco IOS
devices, 164-178
steps of
  DH key exchange, 125-126
  IKEv1 Phase 1 tunnel
    negotiation, 124-125
  packet protection, 126-127
  peer authentication, 126
  summary, 128-129
  traffic after IPsec, 127-128
  traffic before IPsec, 127
verifying, 164-168

IPv4
compared to IPv6, 324-325
security
  best practices, 332-333
  common threats, 333-334

IPv6, 321
address format, 325
  all-nodes multicast addresses,
    328
  all-routers multicast addresses,
    328
  anycast addresses, 328
  configuring, 326-327
  conversion between decimal,
    binary, and hexadecimal, 326
  length, 325
  link-local addresses, 327
  loopback addresses, 327
  solicited-node multicast
    addresses, 328
  unicast addresses, 328
advantages of, 324
compared to IPv4, 324-325
interface information, 328-329
routing, 330-331
security, 332
  ACLs (access control lists), 337
  advantages of IPv6, 334
best practices, 332-333, 336
common threats, 333-334
potential risks, 334-336
ipv6 access-list command, 337, 339
ipv6 address command, 326, 339
ipv6 ospf 1 area 0 command, 339
ipv6 traffic-filter command, 337-339
ipv6 unicast-routing command, 330, 339
ISAKMP (Internet Security Association and Key Management Protocol), 123
ISE (Identity Services Engine), 14, 39, 75
ISPs (Internet service providers), 11
ISR (Integrated Services Routers), 75

K

key loggers, 498
key management
DH key exchange, 125-126
IKE (Internet Key Exchange), 123
key pairs, 93, 99
keyspace, 96
next-generation encryption protocols, 97
overview, 92, 96-97
PKI (public key infrastructure), 99
CAs (certificate authorities), 100-101, 104
components, 114-115
digital signatures, 100
identity certificates, 102
installing digital certificates on ASA, 107-114
key pairs, 99
PKCS (Public Key Cryptography Standards), 105
revoked certificates, 105-106
root certificates, 101-102
RSA algorithm, 99-100
SCEP (Simple Certificate Enrollment Protocol), 105
topologies, 106-107
uses for digital certificates, 106
X.500 certificates, 103
X.509 certificates, 103-104
private keys, 93
PSK (pre-shared keys), 122
public keys, 93, 103
keyspace, 96

L

latent threats, 7
Layer 2 security. See also VLANs (virtual LANs)
best practices, 246-247
CCNA Security
BPDU Guard, 248-249
port security, 250-251
Root Guard, 249
CDP (Cisco Discovery Protocol)
  disabling, 252
  overview, 251-252
DAI (Dynamic ARP Inspection)
  disabling, 252
  overview, 251-252
DHCP (Dynamic Host Configuration Protocol) snooping, 253-254
Layer 2 security toolkit, 248
negotiations, 247
STP (Spanning Tree Protocol)
  learning state, 245
  listening state, 245
  overview, 241-242
Rapid Spanning Tree, 245-246
verification and annotations, 242-245
toolkit, 248
Layer 4 Protocol 50, 153
Layer 4 protocol 51, 153
layered approach to security, 360-361
LDAP (Lightweight Directory Access Protocol), 103
learning state (STP), 245
learningnetwork.cisco.com, 507
least privilege, rule of, 16
length of IPv6 addresses, 325
Lightweight Directory Access Protocol (LDAP), 103
line console 0login authentication bubba command, 318
Link Layer Discovery Protocol (LLDP), 252
link-local addresses, 327
Linux, encryption of endpoint data at rest, 501
listeners, 482
listening state (STP), 245
LLDP (Link Layer Discovery Protocol), 252
LLDP-MED, 252
location of data, 3
locking switch ports, 247
log action, 382
logging
ACL logging, 345
IPS/IDS, 466
overview, 280, 288-289
policy maps, 382
SVC logging, 229
Syslog
configuring, 308-310
security levels, 289
logic bombs, 497
logical controls, 11
login, SSL clientless VPN configuration, 215-216
Login Password Retry Lockout, 279
loopback addresses, 327
mail exchangers (MX), 482
mailconfig command, 485, 493
mailers, 497
malicious traffic, identifying, 463
anomaly-based IPS/IDS, 464-465
policy-based IPS/IDS, 464-465
reputation-based IPS/IDS, 464-465
RR (risk rating), 467-468
sensor responses to detected attacks, 465-467
signature-based IPS/IDS, 464-465
malvertising, 29
malware, 13, 479
antivirus/antimalware solutions, 497-498
Cisco AMP (Advanced Malware Protection) for Endpoints, 31, 499-500
malware identification tools
Cisco AMP (Advanced Malware Protection), 31
IPS events, 31
NetFlow, 30
NGIPS (next-generation intrusion prevention system), 31
packet captures, 30
Snort, 30
man-in-the-middle attacks, 14-15, 333
Management Information Base (MIB), 310

management plane security
AAA (authentication, authorization, and accounting), 279-286
Cisco Secure ACS Solution Engine, 283
components, 282
enabling with method lists, 292-296
method lists, 285-286
overview, 279-281
router access authentication, 284-285
self-contained AAA, 283
troubleshooting, 296-301
VPN user authentication, 283-284
best practices, 278-280
encrypted management protocols, 288
HTTPS, 307-308
logging
overview, 288-289
Syslog configuration, 308-310
syslog security levels, 289
NTP (Network Time Protocol)
configuring, 313-315
defined, 264
overview, 289
security best practices, 267-268
threat control and mitigation strategy, 265
overview, 275, 278
password recommendations, 281, 290-292
RBAC (role-based access control)
custom privilege levels, 287, 301-303
overview, 279, 286
parser views, 287, 303-305
SCP (Secure Copy Protocol), 315
secure bootset
creating, 315-316
overview, 289-290
SNMP (Simple Network Management Protocol), 310-313
authentication, 312
components, 310
configuration, 312-313
encryption, 312
GET message, 310
integrity, 312
security levels, 311-312
security model, 311
SET message, 310
trap message, 311
SSH (Secure Shell)
overview, 287
preparing for, 305-307
management traffic, 278
managers (SNMP), 310
maps
class maps, 381
policy maps, 381-382
mass-mailer worms, 497
match address command, 200
match statements, 381
match-all condition, 381
match-any condition, 381
maximum transmission unit (MTU), 336, 345
MD5 (message digest 5) algorithm
overview, 94-95, 124, 311, 348
routing update authentication
on BGP, 351-352
on EIGRP, 349-350
on OSPF, 348-349
on RIP, 350-351
MDM (mobile device management)
cloud-based deployment, 78-79
on-premise deployment, 77-78
overview, 76
Media Endpoint Device, 252
memory tables, 507
message digest 5 algorithm. See MD5 (message digest 5) algorithm
message-digest keyword, 348
message digests, 94
method lists, 285-286, 292-296
MIB (Management Information Base), 310
micro-engines, 470
minimizing impact of control plane traffic on CPU, 344-345
mirrored VPN configuration, 139
mitigating endpoint threats, 495
antivirus/antimalware solutions, 497-498
Cisco AMP (Advanced Malware Protection) for Endpoints, 31, 499-500
e-mail encryption, 500-501
encryption of endpoint data at rest, 501
HIPS (host intrusion prevention systems), 498
personal firewalls, 498-499
VPNs (virtual private networks), 501-502
mobile device management. See MDM (mobile device management)
Modular Policy Framework (MPF), 424
monitoring alarms/alerts, 471
motivations behind threats, 27
MPF (Modular Policy Framework), 424
MPLS (Multiprotocol Label Switching), 88, 178
MTU (maximum transmission unit), 336, 345
Multiprotocol Label Switching (MPLS), 88, 178
multistring micro-engine, 470
MX (mail exchangers), 482
N
NAC (Network Admission Control), 14
nameif bubba command, 455
nat command, 200
NAT (Network Address Translation)
ASA (Adaptive Security Appliance), 445-447
configuring, 404-407
deployment options, 369-370
dynamic NAT, 369
NAT Exempt policy, 183
NAT with overload, 368
overview, 324, 360, 366-367, 418
PAT (Port Address Translation), 368-369
policy NAT, 370
static NAT, 369
terminology, 367-368
verifying, 407-408
National Vulnerability Database (NVD), 10
native VLAN on trunk, 239
NDP (Neighbor Discovery Protocol), 325, 334
negatives, true/false, 463
negotiations, 228, 247
neighbor cache resource starvation, 334
Neighbor Discovery Protocol (NDP), 325, 228
NetFlow, 30
Network Address Translation. See NAT (Network Address Translation)
Network Admission Control (NAC), 14
network antivirus, 481
network architecture
security guidelines, 16-17
network security
cost-benefit analysis, 7
security terms, 8
network threats. See threats
Network Time Protocol. See NTP (Network Time Protocol)
NFP (Network Foundation Protection)
control plane
defined, 264
explained, 268
security best practices, 268-269
thr threat control and mitigation strategy, 265
data plane
additional protection mechanisms, 271
defined, 264
explained, 270
security best practices, 271
threat control and mitigation strategy, 266
framework, 264
importance of, 264
interdependence, 265
management plane
defined, 264
security best practices, 267-268
threat control and mitigation strategy, 265
overview, 261, 264
threat control and mitigation strategy, 265-266
NFS (Network File System), 15
NGE (next-generation encryption), 97, 124
NGFW (next-generation firewalls), 365
NGIPS (next-generation intrusion prevention system), 31, 472-473
no cdp enable command, 259
no cdp run command, 259
no debug aaa authentication command, 296
no shutdown command, 330, 420, 455
No Telnet policy, verifying, 453
noAuthNoPriv security level, 311
nondesignated ports, 245
NTP (Network Time Protocol), 28, 102, 267, 280, 289, 332
configuring, 156, 313-315
verifying status of, 157
NVD (National Vulnerability Database), 10

O
Oakley, 123
object groups, 418
object network command, 200
obtaining digital certificate, 158-159
OCSP (Online Certificate Status Protocol), 106
on-premise MDM (mobile device management) deployment, 77-78
one-time password (OTP), 76, 92
Online Certificate Status Protocol (OCSP), 106
OOB (out-of-band) management, 267, 279
Open Shortest Path First (OSPF), 268, 348-349
orphaned rules, 373
OSPF (Open Shortest Path First), 268, 348-349
Other micro-engine, 470
OTP (one-time password), 76, 92
out-of-band (OOB) management, 267, 279
outbreak filters, 481
outside global NAT (Network Address Translation), 367
outside local NAT (Network Address Translation), 367
overload, NAT (Network Address Translation) with, 368

P
PAC (proxy autoconfiguration), 486
packet amplification attacks, 335
packet captures, 30
packet filtering
  access rule structure, 372
  ASA (Adaptive Security Appliance)
    packet-filtering ACLs, 423
    packet filtering on ASA, 422-423
explained, 417
  stateful packet filtering, 363-364
  static packet filtering, 362
packet mode, 284
packet protection (IPsec), 126-127
Packet Tracer, 449-453
pads, 92
parser views, 287, 303-305
pass action, 382
password-guessing attacks, 15
passwords, 29
  management plane security, 281, 290-292
  password-guessing attacks, 15
  strong passwords, 279-281, 290-292
PAT (Port Address Translation), 209, 368-369, 445-447
PCPT (Pearson Cert Practice Test) software, 506
Pearson Cert Practice Test engine
  installing, 505
  practice exam mode, 508-509
  study mode, 508
Pearson Cert Practice Test (PCPT) software, 506
peer authentication, 126
peer device identification, 180
personal firewalls, 355, 498-499
personally identifiable information (PII), 31
pharming, 13
phishing, 13, 29, 479
phone scams, 29
physical controls, 11
physical security, 30, 332
PII (personally identifiable information), 31
ping command, 60, 165-170
PIX, 413
PKCS (Public Key Cryptography Standards), 94, 105
PKI (public key infrastructure), 99, 207, 434
CAs (certificate authorities)
  authenticating and enrolling with, 104
  explained, 100-101
digital signatures, 100
identity certificates, 102
installing digital certificates on ASA, 107
default certificate, 108
identity certificates, 111-114
root certificates, 109-114
key pairs, 99
PKCS (Public Key Cryptography Standards), 105
revoked certificates, 105-106
root certificates, 101-102
RSA algorithm, 99-100
SCEP (Simple Certificate Enrollment Protocol), 105
topologies, 106-107
uses for digital certificates, 106
X.500 certificates, 103
X.509 certificates, 103-104
planning IPsec site-to-site VPNs, 129
customer needs, 152-153
IKEv1 Phase 1 planning, 154
IKEv1 Phase 2 planning, 154-155
required protocols, 153
point-of-sale (PoS) systems, 27
poisoning (ARP), 271
policies
ASA (Adaptive Security Appliance)
  MPF (Modular Policy Framework), 424
  policy application, 425
authorization policies, 56-57
MPF (Modular Policy Framework), 424
policy-based IPS/IDS, 464-465
policy maps, 381-382
service policies, 333, 382-384
policy-map type inspect command, 410
policy maps, 381-382
policy NAT (Network Address Translation), 370
polyalphabetic ciphers, 91
Port Address Translation (PAT), 209, 368-369, 445-447
PortFast, 245-246
ports
PAT (Port Address Translation), 209, 368-369, 445-447
root ports, 244
security, 250-251
switch ports
  BPDU Guard, 248
  locking down, 247
  recovery of err-disabled ports, 249
trunk ports, 238-239
RIP routing update authentication

PoS (point-of-sale) systems, 27
positives, true/false, 463
potential attackers, 12
practice configurations, 508
practice exam
activating and downloading, 506
practice exam mode (Pearson Cert
Practice Test engine), 508-509
Premium Edition, 506
Premium Edition, 506
preparation
for HTTPS, 307-308
for SSH (Secure Shell), 305-307
pre-shared keys (PSK), 122, 125
private keys, 93
private listeners, 482
privilege escalation, 13
privilege exec level command, 302, 318
privilege levels (RBAC), 287, 301-303
profiles
authorization profiles, 58-60
connection profile access, 211
connection profiles
Cisco AnyConnect Secure
Mobility Client, 225-226
IPsec site-to-site VPNs, 189-191
protocol level misinterpretation, 469
proxy autoconfiguration (PAC), 486
proxy firewalls, 363
PSK (pre-shared keys), 122, 125
Public Key Cryptography Standards
(PKCS), 94, 105
public key infrastructure. See PKI
(public key infrastructure)
public keys, 93, 103
public listeners, 482
Q-R
QoS (quality of service), 269
Quick Setup Wizard (IPsec), 129-130
RADIUS (Remote Authentication Dial-
In User Service), 39-40
ransomware, 498
Rapid Spanning Tree (RSP), 245-246
RBAC (role-based access control), 267, 287
custom privilege levels, 287, 301-303
overview, 279, 286
parser views, 287, 303-305
RRDoS (reflected DDoS) attack, 16
Real-time Transport Protocol (RTP), 424
realized threats, 7
reconnaissance, 13
recovery of err-disabled ports, 249
RED classification level (TLP), 9
redundant rules, 373
reflected DDoS (RRDoS) attack, 16
reflected DoS (denial-of-service) attacks, 28
remote-access VPNs (virtual private networks), 88, 502
Remote Authentication Dial-In User
Service (RADIUS), 39-40
reputation-based IPS/IDS, 464-465
resetting TCP connections, 467
resource exhaustion, 469
revoked certificates, 105-106
RH0, 336
RIP routing update authentication,
350-351
risk management

defined, 7-8
overview, 11
RR (risk rating), 467-468
role-based access control. See RBAC (role-based access control)
root bridge, 242
root certificates, 101-102, 109-114
Root Guard, 249
root ports, 244
rootkits, 498
route processor (RP), 269
router-on-a-stick, 240-241
routers. See also routing
access authentication, 284-285
configuration for ACS
AAA verification, 43-45
CCP (Cisco Configuration Professional), 45-50
CLI (command line interface), 41-43
overview, 41
TACACS+, 45
control plane security
CoPP (control plane policing), 346-347
CPPr (control plane protection), 348
impact of control plane traffic on CPU, minimizing, 344-345
overview, 344
routing update authentication on BGP, 351-352
routing update authentication on EIGRP, 349-350
routing update authentication on OSPF, 348-349
routing update authentication on RIP, 350-351
router-on-a-stick, 240-241
router-to-ACS interactions, 60
basic connectivity, 60
debug command, 62-66
ping command, 60
test command, 60-62
routing. See also routers
ASA (Adaptive Security Appliance), 444-445
IPv6, 330-331
routing protocols authentication, 269
routing update authentication
on BGP, 351-352
on EIGRP, 349-350
on OSPF, 348-349
on RIP, 350-351
RP (route processor), 269
RR (risk rating), 467-468
RSA algorithm, 94, 99-100
RSA SecurID, 76
rsa-signatures, 96
RSP (Rapid Spanning Tree), 245-246
RTP (Real-time Transport Protocol), 424
rule implementation
access rules, 447-449
firewalls, 373-374
rule of least privilege, 16

S

SA (security associations), 129
sandboxing, 491
SCEP (Simple Certificate Enrollment Protocol), 105
SCP (Secure Copy Protocol), 315
script-kiddies, 12
SDEE (Security Device Event Exchange), 471
secure boot-config command, 316
secure boot-image command, 316-318
secure bootset
  creating, 315-316
  overview, 289-290
Secure Copy Protocol (SCP), 315
Secure Hash Algorithm (SHA), 124, 311
Secure Hash Algorithm 1 (SHA-1), 95
Secure Hash Algorithm 2 (SHA-2), 95
Secure Key Exchange Mechanism (SKEME), 123
Secure/Multipurpose Internet Mail Extensions (S/MIME), 500
Secure Neighbor Discovery in IPv6 (SeND), 336
Secure Shell. See SSH (Secure Shell)
Secure Sockets Layer. See SSL (Secure Sockets Layer)
security associations (SA), 129
Security Device Event Exchange (SDEE), 471
security intelligence, 471-472
Security Intelligence Operations (SIO), 472, 481
security-level 50 command, 455
security levels (ASA), 419-420
Security Management Appliance (SMA), 491-492
security model, 311
security passwords min-length command, 281
security policies. See policies
security terms, 8
Selective Packet Discard (SPD), 269
self-contained AAA, 283
self zones, 380, 384-385
SeND (Secure Neighbor Discovery in IPv6), 336
Sender ID Framework (SIDF), 481
Sender Policy Framework (SPF), 481
SenderBase, 481
sensors
  defined, 460
  responses to detected attacks, 465-467
  sensor platforms, 462
separation of duties, 16
serial numbers (digital certificates), 102-103
servers. See ACS (Access Control Server)
service micro-engine, 470
service password-encryption command, 291, 318
service policies, 382-384
SET message, 310
set peer command, 200
setup script (ASA), 432-433
severity levels, 470-471
SFR (signature fidelity rating), 467, 471
SHA (Secure Hash Algorithm), 124, 311
SHA-1 (Secure Hash Algorithm 1), 95
SHA-2 (Secure Hash Algorithm 2), 95
shadowed rules, 373
show class-map type inspect command, 401, 410
show command, 327
show crypto ikev1 stats command, 193
show crypto ikev2 stats command, 193
show crypto ipsec sa command, 177, 193-196, 200
show crypto ipsec sa detail command, 193
show crypto isakmp policy command, 142, 162
show crypto isakmp sa command, 176
show crypto isakmp sa detail command, 176
show crypto isakmp stats command, 193
show crypto map command, 142, 147, 175, 200
show errdisable recovery command, 249
show interfaces command, 258
show interfaces trunk command, 244
show ip cef command, 344
show ip nat translations command, 408-410
show ipv6 interface command, 329
show ipv6 protocol command, 331
show isakmp sa command, 193
show isakmp sa detail command, 193, 196-197, 200
show isakmp stats command, 193-195, 200
show ntp association command, 157, 314
show ntp status command, 157, 314
show policy-map control-plane command, 346-347
show policy-map type inspect command, 410
show policy-map type inspect zone-pair ccp-zp-in-out sessions command, 402
show secure bootset command, 316
show spanning-tree vlan 10 command, 242-243, 246
show vpn-sessiondb command, 193, 197, 201
SIDF (Sender ID Framework), 481
signature-based IPS/IDS, 464-465
signature fidelity rating (SFR), 467, 471
signatures. See digital signatures
Simple Certificate Enrollment Protocol (SCEP), 105
Simple Mail Transfer Protocol (SMTP), 481
single root CA (certificate authority), 107
SIO (Security Intelligence Operations), 472, 481
site-to-site VPN (virtual private network)
alternatives to, 178
customer needs, 152-155
implementing in Cisco ASA, 179-192
  commands sent to Cisco ASA, 184-189
  connection profiles, 189-191
  IKE policy, 191
  IKEv1 policies, 191
  IKEv2 settings, 192
  IPsec proposals (transform sets), 192
  local/remote networks, 181-182
  NAT Exempt policy, 183
  peer device identification, 180
  security options, 182
  traffic to protect, 180-181
implementing in Cisco IOS devices, 155-164
  crypto policy, 162-164
  digital certificates, 158-159
  NPT configuration, 156
  NPT status verification, 157
  Site-to-Site VPN Wizard, 159-162
overview, 88, 149, 502
required protocols, 153
troubleshooting in Cisco ASA, 193-198
debug command, 198
show crypto ipsec sa command, 195-196
show crypto isakmp stats command, 193
show isakmp sa detail command, 196-197
show isakmp stats command, 193-195
show vpn-sessiondb command, 197
troubleshooting in Cisco IOS devices, 164-178
debug command, 165-166
IKEv1 Phase 1 policy, 170-174
IKEv1 Phase 2 policy, 174-178
ping command, 165-170
verification of IPSec configuration, 164-168
Site-to-Site VPN Wizard, 159-162, 179-184
SKEME (Secure Key Exchange Mechanism), 123
SMA (Security Management Appliance), 491-492
small office/home office (SOHO), 18
S/MIME (Secure/Multipurpose Internet Mail Extensions), 500
SMTP (Simple Mail Transfer Protocol), 481
sniffing, 333
SNMP (Simple Network Management Protocol), 288, 310-313
authentication, 312
components, 310
configuration, 312-313
encryption, 312
GET message, 310
integrity, 312
security levels, 311-312
security model, 311
SET message, 310
traps, 311, 467
snmp-server group command, 319
snmp-server host command, 319
snmp-server user command, 319
snooping (DHCP), 253-254
Snort, 30
social engineering, 13, 28-30
defenses against, 29-30
malvertising, 29
phishing, 29
phone scams, 29
SOHO (small office/home office), 18
solicited-node multicast addresses, 328
spam, 479, 497
spanning-tree bpduguard enable command, 258
spanning-tree guard root command, 249, 259
spanning-tree mode rapid-pvst command, 246
spanning-tree portfast command, 245
spanning-tree portfast default command, 245
Spanning Tree Protocol. See STP (Spanning Tree Protocol)
SPD (Selective Packet Discard), 269
spear phishing, 479
SPF (Sender Policy Framework), 481
split tunneling, 227-228
spoofing
ARP spoofing, 271
spoofed packets, 334
SSH (Secure Shell)
overview, 15, 287, 332
preparing for, 305-307
SSL (Secure Sockets Layer)
Cisco AnyConnect Secure Mobility
Client, 217
click profiles, 225-226
full-tunnel SSL VPN
configuration, 218-225
groups, 225-226
split tunneling, 227-228
tunnel groups, 226
types of SSL VPNs, 218
compared to IPsec (IP security), 206
compared to TLS (Transport Layer
Security), 207
defined, 88
how it works, 207-208
overview, 98, 203
SSL clientless VPN configuration
CLI (command line interface),
214-215
click profile access, 211
digital certificates, 211
login, 215-216
SSL VPN Wizard, 209-210
user authentication, 211-214
VPN statistics, 217
SSL VPN access methods, 208-209
troubleshooting
initial connectivity issues,
228-229
negotiations, 228
traffic-specific issues, 230
SSL VPN Wizard, 209-210
stateful database, 364
stateful filtering 363-364, 417
states
stateful database, 364
stateful filtering 363-364, 417
STP (Spanning Tree Protocol), 245
static NAT (Network Address
Translation), 369
static packet filtering, 362
statistics (VPN), viewing, 217
status (NTP), verifying, 157
Step by Step VPN Wizard (IPsec),
130-137
STP (Spanning Tree Protocol)
learning state, 245
listening state, 245
overview, 14, 241-242, 333
RSP (Rapid Spanning Tree), 245-246
verification and annotations, 242-245
stream ciphers, 92
string micro-engine, 470
strong passwords, 290-292
study mode (Pearson Cert Practice
Test engine), 508
study plan, 507-509
exam engine, 508-509
practice configurations, 508
recalling the facts, 507-508
subinterfaces, 348
substitution, 91
Summary screen (Cisco AnyConnect
Secure Mobility Client Wizard),
223-224
SVC logging, 229
switch ports
BPDU Guard, 248
locking down, 247
recovery of err-disabled ports, 249
switchport access vlan command, 237,
247, 258
threats  565

switchport mode access command, 237, 247, 258
switchport mode trunk command, 247, 258
switchport nonegotiate command, 247, 258
switchport port-security command, 250, 259
switchport trunk encapsulation dot1q command, 247, 258
switchport trunk native vlan command, 247, 258
symmetric algorithms, 93
symmetric ciphers, 93
symmetrical access lists, 136
syslog, 267
  configuring, 308-310
  overview, 288
  security levels, 289
systemsetup command, 483-485, 493

tacacs-server host command, 42, 45, 68
TACACS+ (Terminal Access Control Access Control Server), 39-40, 45
tags, 238
target value rating (TVR), 467
TCP (Transfer Control Protocol), 360, 384
  resetting connections, 467
  TCP Intercept, 270-271
technical controls, 11
Terminal Access Control Access Control Server (TACACS+), 39-40, 45
test aaa command, 298
test aaa group tacacs+ command, 68
test command, 60-62
threat agents, 7
threat control and mitigation strategy
threat vector, 7
ThreatGRID, 500
threats, 27
attacks
  attack vectors, 14
  back doors, 13
  botnets, 15
  brute-force attacks, 15
  code execution attacks, 13
  covert channel, 15
  data loss and exfiltration methods, 31-32
  DDoS (distributed denial-of-service) attacks, 16, 27-28
  DoS (denial-of-service) attacks, 16, 27-28
  malware identification tools, 30-31
  man-in-the-middle attacks, 14-15
  NFP (Network Foundation Protection), 265-266
  pharming, 13
  phishing, 13
  potential attackers, 12
  privilege escalation, 13
  reconnaissance, 13
  social engineering, 13, 28-30
  trust exploitation, 15
defined, 7-8
e-mail-based threats
  Cisco cloud e-mail security, 479
  Cisco ESA (E-mail Security Appliance), 480-485
  Cisco hybrid e-mail security, 480
  malware attachments, 479
566 threats

phishing, 479
spam, 479
spear phishing, 479
IPv4/IPv6 threats, 333-336
latent threats, 7
motivation behind, 27
realized threats, 7
threat agents, 7
threat vector, 7
web-based threats
Cisco CWS (Cloud Web Security), 486
Cisco SMA (Security Management Appliance), 491-492
Cisco WSA (Web Security Appliance), 487-491
Time-To-Live (TTL), 335, 345
timing attacks, 469
TLP (Traffic Light Protocol), 9-10
TLS (Transport Layer Security), 98, 207
topologies, 17-18
CAN (Campus Area Network), 17
Cloud/WAN (Wide Area Network), 18
Data Center network, 18-19
PKI (public key infrastructure), 106-107
SOHO (small office/home office), 18
ToS (type of service), 30
traffic
ASA (Adaptive Security Appliance), 420-422
before/after IPsec, 127-128
fragmentation, 468
impact of control plane traffic on CPU, 344-345
management traffic, 278
substitution and insertion, 468
troubleshooting, 230
Traffic Light Protocol (TLP), 9-10
Transfer Control Protocol (TCP), 360, 384
transform sets, 126, 192
transparent firewalls, 365
Transport Layer Security. See TLS (Transport Layer Security)
transposition, 91
trap messages, 311
Triple DES (3DES), 124
Triple Digital Encryption Standard (3DES), 94
Trojan horses, 497
troubleshooting
AAA (authentication, authorization, and accounting), 296-301
ACS (Access Control Server)
  basic connectivity, 60
debug command, 62-66
ping command, 60
test command, 60-62
IPsec site-to-site VPNs in Cisco ASA, 193-198
debug command, 198
show crypto isakmp stats command, 193
show crypto isakmp sa detail command, 196-197
show crypto isakmp stats command, 193-195
show vpn-sessiondb command, 197
IPsec site-to-site VPNs in Cisco IOS, 164-178
debug command, 165-166
IKEv1 Phase 1 policy, 170-174
IKEv1 Phase 2 policy, 174-178
ping command, 165-170
verification of IPsec configuration, 164-168
SSL (Secure Sockets Layer)
initial connectivity issues, 228-229
negotiations, 228
traffic-specific issues, 230
TrueCrypt, 501
true/false negatives, 463
trunk ports, 238-239
inter-VLAN routing, 240
native VLAN on trunk, 239
negotiating trunks between switches, 239
virtual sub interfaces, 240
trust exploitation, 15
TTL (Time-To-Live), 335, 345
tunnel-group command, 200
tunneling, 335, 469
IKEv1 Phase 1 tunnels, 124-125
split tunneling, 227-228
tunnel groups, 226
TVR (target value rating), 467
two-factor authentication, 29
type of service (ToS), 30

UDP (User Datagram Protocol), 267, 384
UDP port 500, 153
UDP port 4500, 153
unauthorized access, 333
undebug all command, 296
unicast addresses, 328
Unicast Reverse Path Forwarding (uRPF), 270
Unicast RPF, 345
URL (uniform resource locator)
filtering, 379
uRPF (Unicast Reverse Path Forwarding), 270
user authentication. See AAA
(authentication, authorization, and accounting)
User Datagram Protocol (UDP), 267, 384
user groups (ACS), 54
username command, 284
user authentication.
UTC (coordinated universal time), 156

V
verbose alerts, 466
verification
AAA (authentication, authorization, and accounting), 43-45
ASA (Adaptive Security Appliance), 453
CoPP (control plane policing), 347
IPsec configuration, 139-145, 164-168
NAT (Network Address Translation), 407-408
NTP status, 157
STP (Spanning Tree Protocol), 242-245
ZBFs (Zone-Based Firewalls)
with CCP (Cisco Configuration Professional), 399-400
from command line, 400-404
views (parser), 287, 303-305
virtual environments, 20-21
virtual LANs. See VLANs (virtual LANs)
Virtual Next-Generation IPS (NGIPSv) for VMware, 473
virtual private networks. See VPNs (virtual private networks)
virtual sub interfaces, 240
virtual terminal line (vty), 374, 288
viruses, 13, 497-498
VLANs (virtual LANs)
creating, 237
defined, 236-237
frame forwarding, 239
inter-VLAN routing, 240
native VLAN on trunk, 239
negotiating trunks between switches, 239
overview, 236, 358
router-on-a-stick, 240-241
trunking with 802.1Q, 238-239
virtual sub interfaces, 240
VPNs (virtual private networks)
benefits of VPNs
  antireplay protection, 90
  authentication, 90
  confidentiality, 89-90
  data integrity, 90
components, 99
cryptography
  algorithms, 91-94
ciphers, 91-93
digital signatures, 95-96
Hasbed Message Authentication Code (HMAC), 95
hashes, 94-95
IPsec. See IPsec
  key management, 96-97
  keys, 92
SSL (Secure Sockets Layer), 98
defined, 87
IPsec site-to-site VPNs
  alternatives to, 178
  customer needs, 152-153
  IKEv1 Phase 1 planning, 154
  IKEv1 Phase 2 planning, 154-155
  implementing in Cisco ASA, 179-192
  implementing in Cisco IOS devices, 155-164
  overview, 149
  required protocols, 153
  troubleshooting in Cisco ASA, 193-198
  troubleshooting in Cisco IOS devices, 164-178
method lists, 285-286
mirrored VPN configuration, 139-141
overview, 8, 73, 119, 501-502
PKI (public key infrastructure)
  CAs (certificate authorities), 100-101, 104
  components, 114-115
digital signatures, 100
  identity certificates, 102
  installing digital certificates on ASA, 107-114
  key pairs, 99
PKCS (Public Key Cryptography Standards), 105
revoked certificates, 105-106
root certificates, 101-102
RSA algorithm, 99-100
SCEP (Simple Certificate Enrollment Protocol), 105
topologies, 106-107
uses for digital certificates, 106
X.500 certificates, 103
X.509 certificates, 103-104
remote-access VPNs, 88, 502
router access authentication, 284-285
SSL (Secure Sockets Layer)
  Cisco AnyConnect Secure Mobility Client, 217-228
  compared to IPsec (IP Security), 206
  compared to TLS (Transport Layer Security), 207
full-tunnel SSL VPN configuration, 218
how it works, 207-208
overview, 203
SSL clientless VPN configuration, 209-217
SSL VPN access methods, 208-209
troubleshooting, 228-230
tunnel groups, 226
types of SSL VPNs, 218
TLS (Transport Layer Security), 207
types of VPNs, 88
user authentication, 283-284
vty (virtual terminal line), 288, 374
vulnerabilities
classifying, 10
defined, 7-8

W

WAN (Wide Area Network), 18
  WAN edge, 79
  WAN module (BYOD), 78
WCCP (Web Cache Communication Protocol), 487
web-based threats, 477, 486
  Cisco CWS (Cloud Web Security), 486
  Cisco SMA (Security Management Appliance), 491-492
  Cisco WSA (Web Security Appliance), 487-491
Web Cache Communication Protocol (WCCP), 487
Web Security Appliance (WSA), 477, 487-491
Welcome screen (Cisco AnyConnect Secure Mobility Client Wizard), 218
whaling, 479
WHITE classification level (TLP), 10
Wide Area Network (WAN), 18
wireless access points (APs), 75
wireless WLAN controllers (WLC), 75
wizards
  Basic Firewall Wizard, 386-388
  Basic NAT Wizard, 405-407
  Cisco AnyConnect Secure Mobility Client Wizard
    authentication method, 220-221
    connection profiles, 218-219
    DNS entries, 221-222
    exemptions from NAT, 222-223
    IP address pool information, 220-221
    protocols to support, 219
    software packages to deploy, 220
    Summary screen, 223-224
    Welcome screen, 218
  Firewall Wizard, 386
  IPsec Quick Setup Wizard, 129-130
  IPsec Step by Step VPN Wizard, 130-137
  Site-to-Site VPN Wizard, 159-162, 179-184
570 wizards

SSL VPN Wizard, 209-210
ZBF Wizard, 389-391
WLAN controllers (WLC), 75
WLC (WLAN controllers), 75
worms, 13, 497
WSA (Web Security Appliance), 477, 487-491

X-Y-Z

X.500 certificates, 103
X.509 certificates, 103-104

ZBFs (Zone-Based Firewalls), 377
C3PL (Cisco Common Classification Policy Language), 381
class maps, 381
components, 383-384
configuring with CCP (Cisco Configuration Professional), 385-391
CLI commands created by CCP, 391-399
CME (Call Manager Express), 388-389
DNS servers, 390
interfaces, 387-388
security level, 388-389
features, 379
how they work, 379
NAT (Network Address Translation)
configuring, 404-407
verifying, 407-408
policy maps, 381-382
self zones, 380, 384-385
service policies, 382-384
traffic interaction between zones, 383
verifying
from command line, 400-404
with CCP (Cisco Configuration Professional), 399-400
zones, 380
ZBF Wizard, 389-391
Zone-Based Firewalls. See ZBFs (Zone-Based Firewalls)
zone-pair security in-to-out source
inside destination outside command, 410
zones, 380-381. See also ZBFs (Zone-Based Firewalls)
self zones, 380, 384-385
zone pairs, 380