



Practice tests



Flash Cards



Review Exercises

CCNP and CCIE Security Core

SCOR 350-701



Study Planner

2nd Edition

ciscopress.com

Omar Santos

FREE SAMPLE CHAPTER |



Companion Website and Pearson Test Prep Access Code

Access interactive study tools on this book's companion website, including practice test software, review exercises, a Key Term flash card application, a study planner, and more!

To access the companion website, simply follow these steps:

1. Go to ciscopress.com/register.
2. Enter the **print book ISBN: 9780138221263**.
3. Answer the security question to validate your purchase.
4. Go to your account page.
5. Click on the **Registered Products** tab.
6. Under the book listing, click on the **Access Bonus Content** link.

When you register your book, your Pearson Test Prep practice test access code will automatically be populated in your account under the Registered Products tab. You will need this code to access the practice test that comes with this book. You can redeem the code at **PearsonTestPrep.com**. Simply choose Pearson IT Certification as your product group and log in to the site with the same credentials you used to register your book. Click the **Activate New Product** button and enter the access code. More detailed instructions on how to redeem your access code for both the online and desktop versions can be found on the companion website.

If you have any issues accessing the companion website or obtaining your Pearson Test Prep practice test access code, you can contact our support team by going to pearsonitp.echelp.org.

This page intentionally left blank

CCNP and CCIE Security Core SCOR 350-701

**Official Cert Guide,
2nd Edition**

OMAR SANTOS

CCNP and CCIE Security Core SCOR 350-701 Official Cert Guide, 2nd Edition

Omar Santos

Copyright © 2024 Cisco Systems, Inc.

Published by:
Cisco Press

All rights reserved. This publication is protected by copyright, and permission must be obtained from the publisher prior to any prohibited reproduction, storage in a retrieval system, or transmission in any form or by any means, electronic, mechanical, photocopying, recording, or likewise. For information regarding permissions, request forms, and the appropriate contacts within the Pearson Education Global Rights & Permissions Department, please visit www.pearson.com/permissions.

No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.

\$PrintCode

Library of Congress Control Number: 2023914718

ISBN-13: 978-0-13-822126-3

ISBN-10: 0-13-822126-X

Warning and Disclaimer

This book is designed to provide information about the Implementing and Operating Cisco Security Core Technologies (SCOR 350-701) exam. Every effort has been made to make this book as complete and accurate as possible, but no warranty or fitness is implied. The information provided is on an “as is” basis. The author and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the supplemental online content or programs accompanying it.

Trademark Acknowledgments

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

Special Sales

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

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact intlcs@pearson.com.

Feedback Information

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

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

We greatly appreciate your assistance.

Vice President, IT Professional: Mark Taub

Copy Editors: Bart Reed and Chuck Hutchinson

Director, ITP Product Management: Brett Bartow

Alliances Manager, Cisco Press: Jaci Featherly;
James Risler

Technical Editor: John Stuppi

Executive Editor: James Manly

Designer: Chuti Prasertsith

Managing Editor: Sandra Schroeder

Composition: codeMantra

Development Editor: Christopher A. Cleveland

Indexer: Erika Millen

Senior Project Editor: Mandie Frank

Proofreader: Donna E. Mulder

Editorial Assistant: Cindy Teeters



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

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

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, visit www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner in this document indicates a partnership relationship between Cisco and any other company. (1110R)

Pearson's Commitment to Diversity, Equity, and Inclusion

Pearson is dedicated to creating bias-free content that reflects the diversity of all learners. We embrace the many dimensions of diversity, including but not limited to race, ethnicity, gender, socioeconomic status, ability, age, sexual orientation, and religious or political beliefs.

Education is a powerful force for equity and change in our world. It has the potential to deliver opportunities that improve lives and enable economic mobility. As we work with authors to create content for every product and service, we acknowledge our responsibility to demonstrate inclusivity and incorporate diverse scholarship so that everyone can achieve their potential through learning. As the world's leading learning company, we have a duty to help drive change and live up to our purpose to help more people create a better life for themselves and to create a better world.

Our ambition is to purposefully contribute to a world where

- Everyone has an equitable and lifelong opportunity to succeed through learning
- Our educational products and services are inclusive and represent the rich diversity of learners
- Our educational content accurately reflects the histories and experiences of the learners we serve
- Our educational content prompts deeper discussions with learners and motivates them to expand their own learning (and worldview)

While we work hard to present unbiased content, we want to hear from you about any concerns or needs with this Pearson product so that we can investigate and address them.

Please contact us with concerns about any potential bias at <https://www.pearson.com/report-bias.html>.

Credits

Figure 1-4: United States Department of Defense

Figure 1-6: Webgoat SQL Injection

Figure 1-1, Figure 1-2: OffSec Services Limited

Figure 3-27-Figure 3-30: Python Software Foundation

Figure 9-11: Amazon Web Services

Figure 9-14-Figure 9-16: Docker Inc

Figure 9-19-Figure 9-21: Google Inc

Figure 10-2: Apple Inc

About the Author

Omar Santos is a cybersecurity thought leader with a passion for driving industry-wide initiatives to enhance the security of critical infrastructures. Omar is the lead of the DEF CON Red Team Village, the chair of the Common Security Advisory Framework (CSAF) technical committee, and board member of the OASIS Open standards organization. Omar's collaborative efforts extend to numerous organizations, including the Forum of Incident Response and Security Teams (FIRST) and the Industry Consortium for Advancement of Security on the Internet (ICASI).

Omar is a renowned expert in ethical hacking, vulnerability research, incident response, and AI security. He employs his deep understanding of these disciplines to help organizations stay ahead of emerging threats. His dedication to cybersecurity has made a significant impact on businesses, academic institutions, law enforcement agencies, and other entities striving to bolster their security measures. Omar is currently leading several Artificial Intelligence (AI) security research efforts at the Cisco Security and Trust Organization (STO).

With over twenty books, video courses, white papers, and technical articles under his belt, Omar's expertise is widely recognized and respected. As a principal engineer at Cisco's Product Security Incident Response Team (PSIRT), Omar not only leads engineers and incident managers in investigating and resolving cybersecurity vulnerabilities, but also actively mentors the next generation of security professionals. You can follow Omar on Twitter @santosomar.

About the Technical Reviewer

John Stuppi, CCIE No. 11154, is a Technical Leader in the Security & Trust Organization (S&TO) at Cisco where he consults Cisco customers on protecting their networks against existing and emerging cyber security threats, risks, and vulnerabilities. Current projects include working with newly acquired entities to integrate them into Cisco's PSIRT Vulnerability Management processes and advising some of Cisco's most strategic customers on vulnerability management and risk assessment. John has presented multiple times on various network security topics at Cisco Live, Black Hat, as well as other customer-facing cyber security conferences. John is also the co-author of the *CCNA Security 210-260 Official Cert Guide* published by Cisco Press. Additionally, John has contributed to the Cisco Security Portal through the publication of white papers, Security Blog posts, and Cyber Risk Report articles. Prior to joining Cisco, John worked as a network engineer for JPMorgan and then as a network security engineer at Time, Inc., with both positions based in New York City. John is also a CISSP (#25525) and holds AWS Cloud Practitioner and Information Systems Security (INFOSEC) Professional Certifications. In addition, John has a BSEE from Lehigh University and an MBA from Rutgers University. John splits his time between Eatontown, New Jersey and Clemson, South Carolina with his wife, son, daughter, and his dog.

Dedication

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

Acknowledgments

I would like to thank the technical editor and my good friend, John Stuppi, for his time and technical expertise.

I would like to thank the Cisco Press team, especially James Manly and Christopher Cleveland, for their patience, guidance, and consideration.

Finally, I would like to thank Cisco and the Cisco Product Security Incident Response Team (PSIRT), Security and Trust Organization for enabling me to constantly learn and achieve many goals throughout all these years.

Contents at a Glance

| | | |
|------------|---|------|
| | Introduction | xxxi |
| Chapter 1 | Cybersecurity Fundamentals | 2 |
| Chapter 2 | Cryptography | 80 |
| Chapter 3 | Software-Defined Networking Security and Network Programmability | 110 |
| Chapter 4 | Authentication, Authorization, Accounting (AAA) and Identity Management | 156 |
| Chapter 5 | Network Visibility and Segmentation | 232 |
| Chapter 6 | Infrastructure Security | 316 |
| Chapter 7 | Cisco Secure Firewall | 410 |
| Chapter 8 | Virtual Private Networks (VPNs) | 490 |
| Chapter 9 | Securing the Cloud | 578 |
| Chapter 10 | Content Security | 638 |
| Chapter 11 | Endpoint Protection and Detection | 672 |
| Chapter 12 | Final Preparation | 696 |
| Chapter 13 | <i>CCNP and CCIE Security Core SCOR (350-701) Exam Updates</i> | 698 |
| Appendix A | Answers to the “Do I Know This Already?” Quizzes and Q&A Sections | 702 |
| | Glossary | 714 |
| | Index | 732 |

Online Element

| | |
|------------|---------------|
| Appendix B | Study Planner |
|------------|---------------|

Contents

| | | |
|------------------|--|----------|
| | Introduction | xxxi |
| Chapter 1 | Cybersecurity Fundamentals | 2 |
| | “Do I Know This Already?” Quiz | 3 |
| | Foundation Topics | 6 |
| | Introduction to Cybersecurity | 6 |
| | Cybersecurity vs. Information Security (InfoSec) | 6 |
| | The NIST Cybersecurity Framework | 7 |
| | Additional NIST Guidance and Documents | 7 |
| | The International Organization for Standardization (ISO) | 8 |
| | Defining What Are Threats, Vulnerabilities, and Exploits | 8 |
| | What Is a Threat? | 8 |
| | What Is a Vulnerability? | 9 |
| | What Is an Exploit? | 10 |
| | Risk, Assets, Threats, and Vulnerabilities | 12 |
| | Defining Threat Actors | 13 |
| | Understanding What Threat Intelligence Is | 14 |
| | Viruses and Worms | 16 |
| | <i>Types and Transmission Methods</i> | 16 |
| | <i>Malware Payloads</i> | 17 |
| | Trojans | 18 |
| | <i>Trojan Types</i> | 18 |
| | <i>Trojan Ports and Communication Methods</i> | 19 |
| | <i>Trojan Goals</i> | 20 |
| | <i>Trojan Infection Mechanisms</i> | 21 |
| | <i>Effects of Trojans</i> | 22 |
| | Distributing Malware | 22 |
| | Ransomware | 23 |
| | Covert Communication | 24 |
| | Keyloggers | 26 |
| | Spyware | 27 |
| | Analyzing Malware | 28 |
| | Static Analysis | 28 |
| | Dynamic Analysis | 29 |

| | |
|---|----|
| Common Software and Hardware Vulnerabilities | 31 |
| Injection Vulnerabilities | 31 |
| SQL Injection | 31 |
| HTML Injection | 33 |
| Command Injection | 33 |
| Authentication-based Vulnerabilities | 33 |
| <i>Credential Brute-Force Attacks and Password Cracking</i> | 34 |
| <i>Session Hijacking</i> | 35 |
| <i>Default Credentials</i> | 35 |
| <i>Insecure Direct Object Reference Vulnerabilities</i> | 35 |
| Cross-site Scripting (XSS) | 36 |
| Cross-site Request Forgery | 38 |
| Server-side Request Forgery | 38 |
| Cookie Manipulation Attacks | 39 |
| Race Conditions | 39 |
| Unprotected APIs | 39 |
| Typical Attacks Against Artificial Intelligence (AI) and Machine Learning | 40 |
| Return-to-LibC Attacks and Buffer Overflows | 41 |
| OWASP Top 10 | 42 |
| Security Vulnerabilities in Open-Source Software | 42 |
| Confidentiality, Integrity, and Availability | 43 |
| What Is Confidentiality? | 43 |
| What Is Integrity? | 45 |
| What Is Availability? | 46 |
| Talking About Availability, What Is a Denial-of-Service (DoS) Attack? | 46 |
| Access Control Management | 48 |
| Cloud Security Threats | 50 |
| Cloud Computing Issues and Concerns | 51 |
| Cloud Computing Attacks | 53 |
| Cloud Computing Security | 53 |
| IoT Security Threats | 54 |
| IoT Protocols | 56 |
| Hacking IoT Implementations | 57 |
| An Introduction to Digital Forensics and Incident Response | 58 |
| ISO/IEC 27002:2013 and NIST Incident Response Guidance | 58 |
| What Is an Incident? | 59 |

| | |
|--|------------------------|
| False Positives, False Negatives, True Positives, and True Negatives | 60 |
| Incident Severity Levels | 60 |
| How Are Incidents Reported? | 61 |
| What Is an Incident Response Program? | 62 |
| The Incident Response Plan | 62 |
| The Incident Response Process | 63 |
| Tabletop Exercises and Playbooks | 65 |
| Information Sharing and Coordination | 66 |
| Computer Security Incident Response Teams | 67 |
| Product Security Incident Response Teams (PSIRTs) | 69 |
| The Common Vulnerability Scoring System (CVSS) | 69 |
| The Stakeholder-Specific Vulnerability Categorization (SSVC) | 73 |
| National CSIRTs and Computer Emergency Response Teams (CERTs) | 74 |
| Coordination Centers | 74 |
| Incident Response Providers and Managed Security Service Providers (MSSPs) | 75 |
| Key Incident Management Personnel | 75 |
| Summary | 76 |
| Exam Preparation Tasks | 76 |
| Review All Key Topics | 76 |
| Define Key Terms | 78 |
| Review Questions | 78 |
| Chapter 2 | Cryptography 80 |
| “Do I Know This Already?” Quiz | 80 |
| Foundation Topics | 82 |
| Introduction to Cryptography | 82 |
| Ciphers | 82 |
| Keys | 83 |
| Block and Stream Ciphers | 84 |
| Symmetric and Asymmetric Algorithms | 84 |
| Hashes | 86 |
| Hashed Message Authentication Code | 89 |
| Digital Signatures | 90 |
| Key Management | 92 |
| Next-Generation Encryption Protocols | 92 |
| IPsec | 93 |

| | |
|---|-----|
| Post-Quantum Cryptography | 93 |
| SSL and TLS | 95 |
| Fundamentals of PKI | 97 |
| Public and Private Key Pairs | 97 |
| More About Keys and Digital Certificates | 97 |
| Certificate Authorities | 98 |
| Root Certificates | 99 |
| Identity Certificates | 101 |
| X.500 and X.509v3 | 101 |
| Authenticating and Enrolling with the CA | 102 |
| Public Key Cryptography Standards | 103 |
| Simple Certificate Enrollment Protocol | 103 |
| Revoking Digital Certificates | 103 |
| Digital Certificates in Practice | 104 |
| PKI Topologies | 105 |
| <i>Single Root CA</i> | 105 |
| <i>Hierarchical CA with Subordinate CAs</i> | 105 |
| <i>Cross-Certifying CAs</i> | 106 |
| Exam Preparation Tasks | 106 |
| Review All Key Topics | 106 |
| Define Key Terms | 107 |
| Review Questions | 107 |

Chapter 3 Software-Defined Networking Security and Network Programmability 110

| | |
|--|-----|
| “Do I Know This Already?” Quiz | 110 |
| Foundation Topics | 112 |
| Software-Defined Networking (SDN) and SDN Security | 112 |
| Traditional Networking Planes | 113 |
| So What’s Different with SDN? | 114 |
| Introduction to the Cisco ACI Solution | 114 |
| VXLAN and Network Overlays | 116 |
| Micro-Segmentation | 118 |
| Open-Source Initiatives | 120 |
| More About Network Function Virtualization | 121 |
| NFV MANO | 123 |
| Contiv | 123 |

| | | |
|------------------|--|------------|
| | ThousandEyes Integration | 124 |
| | Cisco Digital Network Architecture (DNA) | 125 |
| | Cisco DNA Policies | 127 |
| | Cisco DNA Group-Based Access Control Policy | 129 |
| | Cisco DNA IP-Based Access Control Policy | 131 |
| | Cisco DNA Application Policies | 131 |
| | Cisco DNA Traffic Copy Policy | 132 |
| | Cisco DNA Center Assurance Solution | 133 |
| | Cisco DNA Center APIs | 135 |
| | Cisco DNA Security Solution | 135 |
| | Cisco DNA Multivendor Support | 136 |
| | Introduction to Network Programmability | 136 |
| | Modern Programming Languages and Tools | 137 |
| | DevNet | 140 |
| | Getting Started with APIs | 140 |
| | REST APIs | 141 |
| | Using Network Device APIs | 145 |
| | YANG Models | 145 |
| | NETCONF | 147 |
| | RESTCONF | 149 |
| | OpenConfig and gNMI | 151 |
| | Exam Preparation Tasks | 151 |
| | Review All Key Topics | 151 |
| | Define Key Terms | 152 |
| | Review Questions | 152 |
| Chapter 4 | Authentication, Authorization, Accounting (AAA) and Identity Management | 156 |
| | “Do I Know This Already?” Quiz | 157 |
| | Foundation Topics | 160 |
| | Introduction to Authentication, Authorization, and Accounting | 160 |
| | The Principle of Least Privilege and Separation of Duties | 161 |
| | Authentication | 162 |
| | Authentication by Knowledge | 162 |
| | Authentication by Ownership or Possession | 164 |
| | Authentication by Characteristic | 164 |
| | Multifactor Authentication | 165 |

| | |
|---|-----|
| Duo Security | 166 |
| Zero Trust and BeyondCorp | 169 |
| Single Sign-On | 171 |
| JWT | 173 |
| SSO and Federated Identity Elements | 174 |
| Authorization | 177 |
| Mandatory Access Control (MAC) | 177 |
| Discretionary Access Control (DAC) | 178 |
| Role-Based Access Control (RBAC) | 178 |
| Rule-Based Access Control | 178 |
| Attribute-Based Access Control | 179 |
| Accounting | 179 |
| Infrastructure Access Controls | 179 |
| Access Control Mechanisms | 179 |
| AAA Protocols | 182 |
| RADIUS | 182 |
| TACACS+ | 184 |
| Diameter | 186 |
| 802.1X | 188 |
| Network Access Control List and Firewalling | 190 |
| VLAN ACLs | 191 |
| Security Group–Based ACL | 191 |
| Downloadable ACL | 191 |
| Cisco Identity Services Engine (ISE) | 192 |
| Cisco Platform Exchange Grid (pxGrid) | 193 |
| Cisco ISE Context and Identity Services | 195 |
| Cisco ISE Profiling Services | 195 |
| Cisco ISE Identity Services | 198 |
| Cisco ISE Authorization Rules | 199 |
| Cisco TrustSec | 201 |
| Posture Assessment | 203 |
| Change of Authorization (CoA) | 204 |
| Configuring TACACS+ Access | 207 |
| Configuring RADIUS Authentication | 213 |
| Configuring 802.1X Authentication | 215 |
| Additional Cisco ISE Design Tips | 222 |

| | | |
|------------------|---|------------|
| | Advice on Sizing a Cisco ISE Distributed Deployment | 224 |
| | Exam Preparation Tasks | 225 |
| | Review All Key Topics | 225 |
| | Define Key Terms | 226 |
| | Review Questions | 227 |
| Chapter 5 | Network Visibility and Segmentation | 232 |
| | “Do I Know This Already?” Quiz | 233 |
| | Foundation Topics | 236 |
| | Introduction to Network Visibility | 236 |
| | NetFlow | 237 |
| | The Network as a Sensor and as an Enforcer | 238 |
| | What Is a Flow? | 238 |
| | NetFlow for Network Security and Visibility | 241 |
| | NetFlow for Anomaly Detection and DDoS Attack Mitigation | 241 |
| | Data Leak Detection and Prevention | 243 |
| | Incident Response, Threat Hunting, and Network Security Forensics | 243 |
| | Traffic Engineering and Network Planning | 248 |
| | NetFlow Versions | 249 |
| | IP Flow Information Export (IPFIX) | 249 |
| | IPFIX Architecture | 251 |
| | Understanding IPFIX Mediators | 251 |
| | IPFIX Templates | 252 |
| | Option Templates | 253 |
| | Understanding the Stream Control Transmission Protocol (SCTP) | 254 |
| | Exploring Application Visibility and Control and NetFlow | 254 |
| | Application Recognition | 254 |
| | Metrics Collection and Exporting | 255 |
| | NetFlow Deployment Scenarios | 255 |
| | NetFlow Deployment Scenario: User Access Layer | 256 |
| | NetFlow Deployment Scenario: Wireless LAN | 256 |
| | NetFlow Deployment Scenario: Internet Edge | 258 |
| | NetFlow Deployment Scenario: Data Center | 259 |
| | NetFlow Deployment Scenario: NetFlow in Site-to-Site and Remote VPNs | 261 |
| | Cisco Secure Network Analytics and Cisco Secure Cloud Analytics | 263 |
| | Cisco Secure Cloud Analytics | 264 |

| | |
|--|-----|
| On-Premises Monitoring with Cisco Secure Cloud Analytics | 267 |
| Cisco Secure Cloud Analytics Integration with Meraki and Cisco Umbrella | 268 |
| Exploring the Cisco Secure Network Analytics Dashboard | 268 |
| Threat Hunting with Cisco Secure Network Analytics | 270 |
| Cisco Cognitive Intelligence and Cisco Encrypted Traffic Analytics (ETA) | 274 |
| What Is Cisco ETA? | 274 |
| What Is Cisco Cognitive Intelligence? | 274 |
| NetFlow Collection Considerations and Best Practices | 279 |
| Determining the Flows per Second and Scalability | 280 |
| Configuring NetFlow in Cisco IOS and Cisco IOS-XE | 280 |
| Simultaneous Application Tracking | 281 |
| Flexible NetFlow Records | 282 |
| Flexible NetFlow Key Fields | 282 |
| Flexible NetFlow Non-Key Fields | 284 |
| NetFlow Predefined Records | 285 |
| User-Defined Records | 286 |
| Flow Monitors | 286 |
| Flow Exporters | 286 |
| Flow Samplers | 286 |
| Flexible NetFlow Configuration | 286 |
| Configure a Flow Record | 287 |
| Configure a Flow Monitor for IPv4 or IPv6 | 289 |
| Configure a Flow Exporter for the Flow Monitor | 291 |
| Apply a Flow Monitor to an Interface | 293 |
| Flexible NetFlow IPFIX Export Format | 294 |
| Configuring NetFlow in NX-OS | 295 |
| Introduction to Network Segmentation | 296 |
| Data-Driven Segmentation | 297 |
| Application-Based Segmentation | 299 |
| Micro-Segmentation with Cisco ACI | 301 |
| Segmentation with Cisco ISE | 302 |
| The Scalable Group Tag Exchange Protocol (SXP) | 303 |
| SGT Assignment and Deployment | 306 |
| Initially Deploying 802.1X and/or TrustSec in Monitor Mode | 306 |
| Active Policy Enforcement | 306 |
| Cisco ISE TrustSec and Cisco ACI Integration | 310 |

| | |
|--|------------|
| Exam Preparation Tasks | 312 |
| Review All Key Topics | 312 |
| Define Key Terms | 313 |
| Review Questions | 314 |
| Chapter 6 Infrastructure Security | 316 |
| “Do I Know This Already?” Quiz | 317 |
| Foundation Topics | 320 |
| Securing Layer 2 Technologies | 320 |
| VLAN and Trunking Fundamentals | 320 |
| What Is a VLAN? | 321 |
| Trunking with 802.1Q | 323 |
| Let’s Follow the Frame, Step by Step | 325 |
| What Is the Native VLAN on a Trunk? | 326 |
| So, What Do You Want to Be? (Asks the Port) | 326 |
| Understanding Inter-VLAN Routing | 326 |
| What Is the Challenge of Only Using Physical Interfaces? | 326 |
| Using Virtual “Sub” Interfaces | 326 |
| Spanning Tree Fundamentals | 328 |
| The Solution to the Layer 2 Loop | 328 |
| STP Is Wary of New Ports | 331 |
| Improving the Time Until Forwarding | 332 |
| Common Layer 2 Threats and How to Mitigate Them | 333 |
| Do Not Allow Negotiations | 334 |
| Layer 2 Security Toolkit | 334 |
| BPDU Guard | 335 |
| Root Guard | 336 |
| Port Security | 336 |
| CDP and LLDP | 338 |
| DHCP Snooping | 339 |
| Dynamic ARP Inspection | 341 |
| Network Foundation Protection | 343 |
| The Importance of the Network Infrastructure | 343 |
| The Network Foundation Protection Framework | 344 |
| Interdependence | 344 |
| Implementing NFP | 344 |

| | |
|--|-----|
| Understanding and Securing the Management Plane | 345 |
| Best Practices for Securing the Management Plane | 345 |
| Understanding the Control Plane | 347 |
| Best Practices for Securing the Control Plane | 347 |
| Understanding and Securing the Data Plane | 348 |
| Best Practices for Protecting the Data Plane | 349 |
| Additional Data Plane Protection Mechanisms | 349 |
| Securing Management Traffic | 350 |
| What Is Management Traffic and the Management Plane? | 350 |
| NETCONF and RESTCONF vs. SNMP | 350 |
| Beyond the Console Cable | 353 |
| Management Plane Best Practices | 354 |
| Password Recommendations | 356 |
| Using AAA to Verify Users | 357 |
| Router Access Authentication | 357 |
| The AAA Method List | 358 |
| Role-Based Access Control | 359 |
| Custom Privilege Levels | 359 |
| Limiting the Administrator by Assigning a View | 359 |
| Encrypted Management Protocols | 359 |
| Using Logging Files | 360 |
| Understanding NTP | 361 |
| Protecting Cisco IOS, Cisco IOS-XE, Cisco IOS-XR, and Cisco NX-OS Files | 362 |
| Implementing Security Measures to Protect the Management Plane | 362 |
| Implementing Strong Passwords | 362 |
| User Authentication with AAA | 364 |
| Using the CLI to Troubleshoot AAA for Cisco Routers | 369 |
| RBAC Privilege Level/Parser View | 371 |
| Implementing Parser Views | 374 |
| SSH and HTTPS | 375 |
| Implementing Logging Features | 378 |
| Configuring Syslog Support | 378 |
| Configuring NTP | 379 |
| Securing the Network Infrastructure Device Image and Configuration Files | 380 |
| Securing the Data Plane in IPv6 | 381 |

| | |
|---|------------|
| Understanding and Configuring IPv6 | 381 |
| The Format of an IPv6 Address | 383 |
| Understanding the Shortcuts | 383 |
| Did We Get an Extra Address? | 383 |
| IPv6 Address Types | 384 |
| Configuring IPv6 Routing | 386 |
| Moving to IPv6 | 388 |
| Developing a Security Plan for IPv6 | 388 |
| Best Practices Common to Both IPv4 and IPv6 | 388 |
| Threats Common to Both IPv4 and IPv6 | 389 |
| The Focus on IPv6 Security | 390 |
| New Potential Risks with IPv6 | 391 |
| IPv6 Best Practices | 393 |
| IPv6 Access Control Lists | 394 |
| Securing Routing Protocols and the Control Plane | 395 |
| Minimizing the Impact of Control Plane Traffic on the CPU | 395 |
| Details about CoPP | 397 |
| Details about CPPr | 399 |
| Securing Routing Protocols | 399 |
| Implementing Routing Update Authentication on OSPF | 400 |
| Implementing Routing Update Authentication on EIGRP | 401 |
| Implementing Routing Update Authentication on RIP | 401 |
| Implementing Routing Update Authentication on BGP | 402 |
| Exam Preparation Tasks | 404 |
| Review All Key Topics | 404 |
| Define Key Terms | 405 |
| Review Questions | 405 |
| Chapter 7 Cisco Secure Firewall | 410 |
| “Do I Know This Already?” Quiz | 410 |
| Foundation Topics | 413 |
| Introduction to Cisco Secure Firewall | 413 |
| Cisco Firewall History and Legacy | 413 |
| Introducing the Cisco ASA | 414 |
| The Cisco ASA FirePOWER Module | 414 |
| Cisco Secure Firewall: Formerly known as Cisco Firepower Threat Defense (FTD) | 415 |

| | |
|---|-----|
| Cisco Secure Firewall | 415 |
| Cisco Secure Firewall Migration Tool | 415 |
| Cisco Secure Firewall Threat Defense Virtual | 416 |
| Cisco Secure Firewall Cloud Native | 417 |
| Cisco Secure Firewall ISA3000 | 418 |
| Cisco Secure WAF and Bot Protection | 419 |
| SD-WAN, Firewall Capabilities, and the Cisco Integrated Services Routers (ISRs) | 419 |
| Introduction to Cisco Secure Intrusion Prevention (NGIPS) | 421 |
| Surveying the Cisco Secure Firewall Management Center (FMC) | 423 |
| Cisco SecureX | 426 |
| Exploring the Cisco Firepower Device Manager (FDM) | 429 |
| Cisco Defense Orchestrator | 433 |
| Comparing Network Security Solutions That Provide Firewall Capabilities | 435 |
| Deployment Modes of Network Security Solutions and Architectures That Provide Firewall Capabilities | 437 |
| Routed vs. Transparent Firewalls | 437 |
| Security Contexts | 438 |
| Single-Mode Transparent Firewalls | 439 |
| Surveying the Cisco Secure Firewall Deployment Modes | 441 |
| Cisco Secure Firewall Interface Modes | 442 |
| Inline Pair | 445 |
| Inline Pair with Tap | 445 |
| Passive Mode | 446 |
| Passive with ERSPAN Mode | 447 |
| Additional Cisco Secure Firewall Deployment Design Considerations | 447 |
| High Availability and Clustering | 448 |
| Clustering | 450 |
| Implementing Access Control | 452 |
| Implementing Access Control Lists in Cisco ASA | 452 |
| Cisco ASA Application Inspection | 458 |
| To-the-Box Traffic Filtering in the Cisco ASA | 459 |
| Object Grouping and Other ACL Features | 460 |
| Standard ACLs | 461 |
| Time-Based ACLs | 461 |
| ICMP Filtering in the Cisco ASA | 462 |

| | | |
|------------------|--|------------|
| | Network Address Translation in Cisco ASA | 463 |
| | Cisco ASA Auto NAT | 469 |
| | Implementing Access Control Policies in the Cisco Firepower Threat Defense | 469 |
| | Cisco Firepower Intrusion Policies | 472 |
| | Variables | 475 |
| | Platform Settings Policy | 476 |
| | Cisco NGIPS Preprocessors | 476 |
| | Cisco Secure Malware Defense | 478 |
| | Security Intelligence, Security Updates, and Keeping Firepower Software Up to Date | 483 |
| | Security Intelligence Updates | 484 |
| | Keeping Software Up to Date | 484 |
| | Exam Preparation Tasks | 484 |
| | Review All Key Topics | 485 |
| | Define Key Terms | 486 |
| | Review Questions | 486 |
| Chapter 8 | Virtual Private Networks (VPNs) | 490 |
| | “Do I Know This Already?” Quiz | 490 |
| | Foundation Topics | 494 |
| | Virtual Private Network (VPN) Fundamentals | 494 |
| | An Overview of IPsec | 496 |
| | <i>IKEv1 Phase 1</i> | 496 |
| | <i>IKEv1 Phase 2</i> | 498 |
| | NAT Traversal (NAT-T) | 501 |
| | IKEv2 | 501 |
| | SSL VPNs | 503 |
| | Cisco Secure Client Mobility | 504 |
| | Deploying and Configuring Site-to-Site VPNs in Cisco Routers | 506 |
| | Traditional Site-to-Site VPNs in Cisco IOS and Cisco IOS-XE Devices | 506 |
| | Tunnel Interfaces | 508 |
| | GRE over IPsec | 508 |
| | More About Tunnel Interfaces | 510 |
| | Multipoint GRE (mGRE) Tunnels | 512 |
| | DMVPN | 512 |
| | GETVPN | 515 |
| | FlexVPN | 518 |

| | |
|---|-----|
| Debug and Show Commands to Verify and Troubleshoot IPsec Tunnels | 522 |
| Configuring Site-to-Site VPNs in Cisco ASA Firewalls | 528 |
| Step 1: Enable ISAKMP in the Cisco ASA | 529 |
| Step 2: Create the ISAKMP Policy | 529 |
| Step 3: Set Up the Tunnel Groups | 530 |
| Step 4: Define the IPsec Policy | 531 |
| Step 5: Create the Crypto Map in the Cisco ASA | 532 |
| Step 6: Configure Traffic Filtering (Optional) | 534 |
| Step 7: Bypass NAT (Optional) | 534 |
| Step 8: Enable Perfect Forward Secrecy (Optional) | 535 |
| Additional Attributes in Cisco Site-to-Site VPN Configurations | 535 |
| Configuring Remote-Access VPNs in the Cisco ASA | 537 |
| Configuring IPsec Remote-Access VPN in the Cisco ASA | 538 |
| Configuring Clientless Remote Access SSL VPNs in the Cisco ASA | 540 |
| Cisco ASA Remote-Access VPN Design Considerations | 541 |
| Pre-SSL VPN Configuration Steps | 542 |
| Understanding the Remote-Access VPN Attributes and Policy Inheritance Model | 544 |
| Configuring Clientless SSL VPN Group Policies | 544 |
| Configuring the Tunnel Group for Clientless SSL VPN | 545 |
| Configuring User Authentication for Clientless SSL VPN | 546 |
| Enabling Clientless SSL VPN | 548 |
| Configuring WebType ACLs | 549 |
| Configuring Application Access in Clientless SSL VPNs | 550 |
| Configuring Client-Based Remote-Access SSL VPNs in the Cisco ASA | 551 |
| Setting Up Tunnel and Group Policies | 552 |
| Deploying the Cisco Secure Client | 553 |
| Understanding Split Tunneling | 554 |
| Understanding DTLS | 555 |
| Configuring Remote-Access VPNs in Cisco Secure Firewall | 556 |
| Using the Remote Access VPN Policy Wizard | 557 |
| Troubleshooting Cisco Secure Firewall Remote-Access VPN Implementations | 566 |
| Configuring Site-to-Site VPNs in the Cisco Secure Firewall | 567 |
| Cisco SD-WAN | 569 |

Exam Preparation Tasks 573

Review All Key Topics 573

Define Key Terms 574

Review Questions 575

Chapter 9 Securing the Cloud 578

“Do I Know This Already?” Quiz 579

Foundation Topics 581

What Is Cloud and What Are the Cloud Service Models? 581

DevOps, Continuous Integration (CI), Continuous Delivery (CD), and
DevSecOps 583

The Waterfall Development Methodology 583

The Agile Methodology 583

DevOps 586

CI/CD Pipelines 588

The Serverless Buzzword 589

Container Orchestration 592

A Quick Introduction to Containers and Docker 592

Kubernetes 597

Microservices and Micro-Segmentation 602

DevSecOps 603

Describing the Customer vs. Provider Security Responsibility for the Different
Cloud Service Models 605

Patch Management in the Cloud 607

Security Assessment in the Cloud and Questions to Ask Your Cloud
Service Provider 607

Cisco Umbrella 608

The Cisco Umbrella Architecture 609

Secure Internet Gateway 610

Cisco Umbrella Investigate 612

Cisco Secure Email Threat Defense 614

Forged Email Detection 614

Sender Policy Framework 615

Email Encryption 615

Cisco Secure Email Threat Defense for Office 365 615

Cisco Attack Surface Management (Formerly Cisco Secure Cloud
Insights) 616

Cisco Secure Cloud Analytics 618

| | |
|--|-----|
| AppDynamics Cloud Monitoring | 619 |
| Cisco Secure Workload | 622 |
| Cisco Secure Workload Agents | 622 |
| Application Dependency Mapping | 622 |
| Cisco Secure Workload Forensics Feature | 623 |
| Cisco Secure Workload Security Dashboard | 623 |
| Cisco XDR | 627 |
| Introducing the XDR Concept | 627 |
| Exploring the Cisco XDR Solution | 628 |
| Cisco XDR Threat Intelligence and Automation | 632 |
| Exam Preparation Tasks | 632 |
| Review All Key Topics | 633 |
| Define Key Terms | 634 |
| Review Questions | 634 |

Chapter 10 Content Security 638

| | |
|---|-----|
| “Do I Know This Already?” Quiz | 638 |
| Foundation Topics | 641 |
| Content Security Fundamentals | 641 |
| Cisco Async Operating System (AsyncOS) | 642 |
| Cisco Secure Web Appliance | 642 |
| The Cisco Secure Web Appliance Proxy | 643 |
| Cisco Secure Web Appliance in Explicit Forward Mode | 644 |
| Cisco Secure Web Appliance in Transparent Mode | 646 |
| Configuring WCCP in a Cisco ASA to Redirect Web Traffic to a Cisco Secure Web Appliance | 647 |
| Configuring WCCP on a Cisco Switch | 649 |
| Configuring the Cisco Secure Web Appliance to Accept WCCP Redirection | 650 |
| Traffic Redirection with Policy-Based Routing | 651 |
| Cisco Secure Web Appliance Security Services | 652 |
| Deploying Web Proxy IP Spoofing | 653 |
| Configuring Policies in the Cisco Secure Web Appliance | 653 |
| Cisco Secure Web Appliance Reports | 655 |
| Cisco Secure Email | 658 |
| Reviewing a Few Email Concepts | 658 |
| Cisco Secure Email Deployment | 659 |

| | | |
|-------------------|--|------------|
| | Cisco Secure Email Listeners | 660 |
| | SenderBase | 660 |
| | The Recipient Access Table (RAT) | 661 |
| | Cisco Secure Email Data Loss Prevention | 661 |
| | SMTP Authentication and Encryption | 661 |
| | Domain Keys Identified Mail (DKIM) | 662 |
| | Cisco Content Security Management Appliance (SMA) | 662 |
| | Exam Preparation Tasks | 667 |
| | Review All Key Topics | 668 |
| | Define Key Terms | 668 |
| | Review Questions | 669 |
| Chapter 11 | Endpoint Protection and Detection | 672 |
| | “Do I Know This Already?” Quiz | 672 |
| | Foundation Topics | 674 |
| | Introduction to Endpoint Protection and Detection | 674 |
| | Endpoint Threat Detection and Response (ETDR) and Endpoint Detection and Response (EDR) | 676 |
| | Cisco Secure Endpoint | 676 |
| | Outbreak Control | 677 |
| | IP Blacklists and Whitelists | 681 |
| | Cisco Secure Endpoint Application Control | 683 |
| | Exclusion Sets | 684 |
| | Cisco Secure Endpoint Connectors | 687 |
| | Cisco Secure Endpoint Policies | 687 |
| | Cisco Secure Client AMP Enabler | 688 |
| | Cisco Secure Endpoint Engines | 689 |
| | Cisco Secure Endpoint Reporting | 690 |
| | Cisco Threat Response | 693 |
| | Exam Preparation Tasks | 693 |
| | Review All Key Topics | 693 |
| | Define Key Terms | 694 |
| | Review Questions | 694 |
| Chapter 12 | Final Preparation | 696 |
| | Hands-on Activities | 696 |
| | Suggested Plan for Final Review and Study | 696 |
| | Summary | 697 |

Chapter 13 CCNP and CCIE Security Core SCOR (350-701) Exam Updates 698

The Purpose of This Chapter 698

About Possible Exam Updates 698

Impact on You and Your Study Plan 699

News about the Next Exam Release 700

Updated Technical Content 700

Appendix A Answers to the “Do I Know This Already?” Quizzes and Q&A Sections 702

Glossary 714

Index 732

Online Element

Appendix B Study Planner

Introduction

The Implementing and Operating Cisco Security Core Technologies (SCOR 350-701) exam is the required “core” exam for the CCNP Security and CCIE Security certifications. If you pass the SCOR 350-701 exam, you also obtain the Cisco Certified Specialist–Security Core Certification. This exam covers core security technologies, including cybersecurity fundamentals, network security, cloud security, identity management, secure network access, endpoint protection and detection, and visibility and enforcement.

The Implementing and Operating Cisco Security Core Technologies (SCOR 350-701) is a 120-minute exam.

TIP You can review the exam blueprint from Cisco’s website at <https://learningnetwork.cisco.com/s/scor-exam-topics>.

This book gives you the foundation and covers the topics necessary to start your CCNP Security or CCIE Security journey.

The CCNP Security Certification

The CCNP Security certification is one of the industry’s most respected certifications. In order for you to earn the CCNP Security certification, you must pass two exams: the SCOR exam covered in this book (which covers core security technologies) and one security concentration exam of your choice, so you can customize your certification to your technical area of focus.

TIP The SCOR core exam is also the qualifying exam for the CCIE Security certification. Passing this exam is the first step toward earning both of these certifications.

The following are the CCNP Security concentration exams:

- Securing Networks with Cisco Firepower (SNCF 300-710)
- Implementing and Configuring Cisco Identity Services Engine (SISE 300-715)
- Securing Email with Cisco Email Security Appliance (SESA 300-720)
- Securing the Web with Cisco Web Security Appliance (SWSA 300-725)
- Implementing Secure Solutions with Virtual Private Networks (SVPN 300-730)
- Automating Cisco Security Solutions (SAUTO 300-735)

TIP CCNP Security now includes automation and programmability to help you scale your security infrastructure. If you pass the Developing Applications Using Cisco Core Platforms and APIs v1.0 (DEVCOR 350-901) exam, the SCOR exam, and the Automating Cisco Security Solutions (SAUTO 300-735) exam, you will achieve the CCNP Security and DevNet Professional certifications with only three exams. Every exam earns an individual Specialist certification, allowing you to get recognized for each of your accomplishments, instead of waiting until you pass all the exams.

There are no formal prerequisites for CCNP Security. In other words, you do not have to pass the CCNA Security or any other certifications in order to take CCNP-level exams. The same goes for the CCIE exams. On the other hand, CCNP candidates often have three to five years of experience in IT and cybersecurity.

Cisco considers ideal candidates to be those that possess the following:

- Knowledge of implementing and operating core security technologies
- Understanding of cloud security
- Hands-on experience with Cisco Secure Firewalls, intrusion prevention systems (IPSs), and other network infrastructure devices
- Understanding of content security, endpoint protection and detection, and secure network access, visibility, and enforcement
- Understanding of cybersecurity concepts with hands-on experience in implementing security controls

The CCIE Security Certification

The CCIE Security certification is one of the most admired and elite certifications in the industry. The CCIE Security program prepares you to be a recognized technical leader. In order to earn the CCIE Security certification, you must pass the SCOR 350-701 exam and an 8-hour, hands-on lab exam. The lab exam covers very complex network security scenarios. These scenarios range from designing through deploying, operating, and optimizing security solutions.

Cisco considers ideal candidates to be those who possess the following:

- Extensive hands-on experience with Cisco's security portfolio
- Experience deploying Cisco Secure Firewalls and IPS devices
- Experience with cloud security solutions
- Deep understanding of secure connectivity and segmentation solutions
- Hands-on experience with infrastructure device hardening and infrastructure security
- Configuring and troubleshooting identity management, information exchange, and access control
- Deep understanding of advanced threat protection and content security

The Exam Objectives (Domains)

The Implementing and Operating Cisco Security Core Technologies (SCOR 350-701) exam is broken down into six major domains. The contents of this book cover each of the domains and the subtopics included in them, as illustrated in the following descriptions.

The following table breaks down each of the domains represented in the exam.

| Domain | Percentage of Representation in Exam |
|---|--------------------------------------|
| 1: Security Concepts | 25% |
| 2: Network Security | 20% |
| 3: Securing the Cloud | 15% |
| 4: Content Security | 15% |
| 5: Endpoint Protection and Detection | 10% |
| 6: Secure Network Access, Visibility, and Enforcement | 15% |
| | Total 100% |

Here are the details of each domain:

Domain 1: Monitoring and Reporting: This domain is covered in Chapters 1, 2, 3, and 8.

- 1.1 Explain common threats against on-premises and cloud environments
 - 1.1.a On-premises: viruses, trojans, DoS/DDoS attacks, phishing, rootkits, man-in-the-middle attacks, SQL injection, cross-site scripting, malware
 - 1.1.b Cloud: data breaches, insecure APIs, DoS/DDoS, compromised credentials
- 1.2 Compare common security vulnerabilities such as software bugs, weak and/or hard-coded passwords, SQL injection, missing encryption, buffer overflow, path traversal, cross-site scripting/forgery
- 1.3 Describe functions of the cryptography components such as hashing, encryption, PKI, SSL, IPsec, NAT-T IPv4 for IPsec, pre-shared key, and certificate-based authorization
- 1.4 Compare site-to-site VPN and remote access VPN deployment types such as sVTI, IPsec, Cryptomap, DMVPN, FLEXVPN, including high availability considerations, and AnyConnect
- 1.5 Describe security intelligence authoring, sharing, and consumption
- 1.6 Explain the role of the endpoint in protecting humans from phishing and social engineering attacks
- 1.7 Explain northbound and southbound APIs in the SDN architecture
- 1.8 Explain DNAC APIs for network provisioning, optimization, monitoring, and troubleshooting
- 1.9 Interpret basic Python scripts used to call Cisco Security appliances APIs

Domain 2: Network Security: This domain is covered primarily in Chapters 5, 6, and 7.

- 2.1 Compare network security solutions that provide intrusion prevention and firewall capabilities
- 2.2 Describe deployment models of network security solutions and architectures that provide intrusion prevention and firewall capabilities
- 2.3 Describe the components, capabilities, and benefits of NetFlow and Flexible NetFlow records

- 2.4 Configure and verify network infrastructure security methods (router, switch, wireless)
 - 2.4.a Layer 2 methods (network segmentation using VLANs; Layer 2 and port security; DHCP snooping; Dynamic ARP inspection; storm control; PVLANs to segregate network traffic; and defenses against MAC, ARP, VLAN hopping, STP, and DHCP rogue attacks)
 - 2.4.b Device hardening of network infrastructure security devices (control plane, data plane, and management plane)
- 2.5 Implement segmentation, access control policies, AVC, URL filtering, and malware protection
- 2.6 Implement management options for network security solutions such as intrusion prevention and perimeter security (single vs. multidevice manager, in-band vs. out-of-band, CDP, DNS, SCP, SFTP, and DHCP security and risks)
- 2.7 Configure AAA for device and network access (authentication and authorization, TACACS+, RADIUS and RADIUS flows, accounting, and dACL)
- 2.8 Configure secure network management of perimeter security and infrastructure devices such as SNMPv3, NETCONF, RESTCONF, APIs, secure syslog, and NTP with authentication
- 2.9 Configure and verify site-to-site VPN and remote access VPN
 - 2.9.a Site-to-site VPN utilizing Cisco routers and IOS
 - 2.9.b Remote-access VPN using Cisco AnyConnect Secure Mobility client
 - 2.9.c Debug commands to view IPsec tunnel establishment and troubleshooting

Domain 3: Securing the Cloud: This domain is covered primarily in Chapter 9.

- 3.1 Identify security solutions for cloud environments
 - 3.1.a Public, private, hybrid, and community clouds
 - 3.1.b Cloud service models: SaaS, PaaS, and IaaS (NIST 800-145)
- 3.2 Compare the customer vs. provider security responsibility for the different cloud service models
 - 3.2.a Patch management in the cloud
 - 3.2.b Security assessment in the cloud
 - 3.2.c Cloud-delivered security solutions such as firewall, management, proxy, security intelligence, and CASB
- 3.3 Describe the concept of DevSecOps (CI/CD pipeline, container orchestration, and security)
- 3.4 Implement application and data security in cloud environments
- 3.5 Identify security capabilities, deployment models, and policy management to secure the cloud
- 3.6 Configure cloud logging and monitoring methodologies
- 3.7 Describe application and workload security concepts

Domain 4: Content Security: This domain is covered primarily in Chapter 10.

- 4.1 Implement traffic redirection and capture methods
- 4.2 Describe web proxy identity and authentication, including transparent user identification
- 4.3 Compare the components, capabilities, and benefits of local and cloud-based email and web solutions (ESA, CES, WSA)
- 4.4 Configure and verify web and email security deployment methods to protect on-premises and remote users (inbound and outbound controls and policy management)
- 4.5 Configure and verify email security features such as SPAM filtering, antimalware filtering, DLP, blacklisting, and email encryption
- 4.6 Configure and verify secure Internet gateway and web security features such as blacklisting, URL filtering, malware scanning, URL categorization, web application filtering, and TLS decryption
- 4.7 Describe the components, capabilities, and benefits of Cisco Umbrella
- 4.8 Configure and verify web security controls on Cisco Umbrella (identities, URL content settings, destination lists, and reporting)

Domain 5: Endpoint Protection and Detection: This domain is covered primarily in Chapter 11.

- 5.1 Compare Endpoint Protection Platforms (EPPs) and Endpoint Detection & Response (EDR) solutions
- 5.2 Explain antimalware, retrospective security, Indicator of Compromise (IOC), antivirus, dynamic file analysis, and endpoint-sourced telemetry
- 5.3 Configure and verify outbreak control and quarantines to limit infection
- 5.4 Describe justifications for endpoint-based security
- 5.5 Describe the value of endpoint device management and asset inventory such as MDM
- 5.6 Describe the uses and importance of a multifactor authentication (MFA) strategy
- 5.7 Describe endpoint posture assessment solutions to ensure endpoint security
- 5.8 Explain the importance of an endpoint patching strategy

Domain 6: Secure Network Access, Visibility, and Enforcement: This domain is covered primarily in Chapters 4 and 5.

- 6.1 Describe identity management and secure network access concepts such as guest services, profiling, posture assessment, and BYOD
- 6.2 Configure and verify network access device functionality such as 802.1X, MAB, and WebAuth
- 6.3 Describe network access with CoA
- 6.4 Describe the benefits of device compliance and application control
- 6.5 Explain exfiltration techniques (DNS tunneling, HTTPS, email, FTP/SSH/SCP/SFTP, ICMP, Messenger, IRC, and NTP)

- 6.6 Describe the benefits of network telemetry
- 6.7 Describe the components, capabilities, and benefits of these security products and solutions:
 - 6.7.a Cisco Secure Network Analytics
 - 6.7.b Cisco Stealthwatch Cloud
 - 6.7.c Cisco pxGrid
 - 6.7.d Cisco Umbrella Investigate
 - 6.7.e Cisco Cognitive Threat Analytics
 - 6.7.f Cisco Encrypted Traffic Analytics
 - 6.7.g Cisco AnyConnect Network Visibility Module (NVM)

Steps to Pass the SCOR Exam

There are no prerequisites for the SCOR exam. However, students must have an understanding of networking and cybersecurity concepts.

Signing Up for the Exam

The steps required to sign up for the Implementing and Operating Cisco Security Core Technologies (SCOR 350-701) exam:

1. Create a Certiport account at <https://www.certiport.com/portal/SSL/Login.aspx>.
2. Once you have logged in, make sure that “Test Candidate” from the drop-down menu is selected.
3. Click on the **Shop Available Exams** button.
4. Select the **Schedule exam** button under the exam you wish to take.
5. Verify your information and continue throughout the next few screens.
6. On the **Enter payment and billing** page, click on **Add Voucher or Promo Code** button if applicable. Enter the voucher number or promo/discount code in the field below and click the **Apply** button.
7. Continue through the next two screens to finish scheduling your exam.

Facts About the Exam

The exam is a computer-based test. The exam consists of multiple-choice questions only. You must bring a government-issued identification card. No other forms of ID will be accepted. You can take the exam at a Pearson Vue center or online via the OnVUE platform. Visit the OnVUE page for your exam program: <https://home.pearsonvue.com/Test-takers/OnVUE-online-proctoring/View-all.aspx>.

Once there, navigate to the FAQs section of the page, where you’ll find helpful information on everything from scheduling your exam to system requirements, testing policies, and more.

TIP Refer to the Cisco Certification site at <https://cisco.com/go/certifications> for more information regarding this, and other, Cisco certifications.

About the CCNP and CCIE Security Core SCOR 350-701 Official Cert Guide

This book maps directly to the topic areas of the SCOR exam and uses a number of features to help you understand the topics and prepare for the exam.

Objectives and Methods

This book uses several key methodologies to help you discover the exam topics that 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. This book does not try to help you pass the exam only by memorization; it seeks to help you to truly learn and understand the topics. This book is designed to help you pass the Implementing and Operating Cisco Security Core Technologies (SCOR 350-701) exam by using the following methods:

- Helping you discover which exam topics you have not mastered
- Providing explanations and information to fill in your knowledge gaps
- Supplying exercises that enhance your ability to recall and deduce the answers to test questions
- Providing practice exercises on the topics and the testing process via test questions on the companion website

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:

- **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 at the end of the chapter:
 - **Review All Key Topics:** The Key Topic icon appears next to the most important items in the “Foundation Topics” section of the chapter. The Review All 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.
 - **Define Key Terms:** Although the Implementing and Operating Cisco Security Core Technologies (SCOR 350-701) exam may be unlikely to ask a question such as “Define this term,” the exam does require that you learn and know a lot of cybersecurity 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.

- **Review Questions:** Confirm that you understand the content you just covered by answering these questions and reading the answer explanations.
- **Web-based practice exam:** The companion website includes the Pearson Cert Practice Test engine, which allows you to take practice exam questions. Use it to prepare with a sample exam and to pinpoint topics where you need more study.

How This Book Is Organized

This book contains 11 core chapters—Chapters 1 through 11. Chapter 12 includes preparation tips and suggestions for how to approach the exam. Each core chapter covers a subset of the topics on the Implementing and Operating Cisco Security Core Technologies (SCOR 350-701) exam. The core chapters map to the SCOR topic areas and cover the concepts and technologies you will encounter on the exam.

The Companion Website for Online Content Review

All the electronic review elements, as well as other electronic components of the book, exist on this book's companion website.

To access the companion website, which gives you access to the electronic content with this book, start by establishing a login at www.ciscopress.com and registering your book.

To do so, simply go to www.ciscopress.com/register and enter the ISBN of the print book: 9780138221263. After you have registered your book, go to your account page and click the **Registered Products** tab. From there, click the **Access Bonus Content** link to get access to the book's companion website.

Note that if you buy the *Premium Edition eBook and Practice Test* version of this book from Cisco Press, your book will automatically be registered on your account page. Simply go to your account page, click the **Registered Products** tab, and select **Access Bonus Content** to access the book's companion website.

Please note that many of our companion content files can be very large, especially image and video files.

If you are unable to locate the files for this title by following the steps above, please visit www.pearsonITcertification.com/contact and select the **Site Problems/Comments** option. Our customer service representatives will assist you.

How to Access the Pearson Test Prep (PTP) App

You have two options for installing and using the Pearson Test Prep application: a web app and a desktop app. To use the Pearson Test Prep application, start by finding the registration code that comes with the book. You can find the code in these ways:

- **Print book or bookseller eBook versions:** You can get your access code by registering the print ISBN (9780138221263) on ciscopress.com/register. Make sure to use the print book ISBN regardless of whether you purchased an eBook or the print book. Once you register the book, your access code will be populated on your account page under the Registered Products tab. Instructions for how to redeem the code are available on the book's companion website by clicking the Access Bonus Content link.

- **Premium Edition:** If you purchase the Premium Edition eBook and Practice Test directly from the Cisco Press website, the code will be populated on your account page after purchase. Just log in at ciscopress.com, click Account to see details of your account, and click the digital purchases tab.

NOTE After you register your book, your code can always be found in your account under the Registered Products tab.

Once you have the access code, to find instructions about both the PTP web app and the desktop app, follow these steps:

- Step 1.** Open this book’s companion website, as shown earlier in this Introduction under the heading “The Companion Website for Online Content Review.”
- Step 2.** Click the **Practice Exams** button.
- Step 3.** Follow the instructions listed there both for installing the desktop app and for using the web app.

Note that if you want to use the web app only at this point, just navigate to pearsontest-prep.com, log in using the same credentials used to register your book or purchase the Premium Edition, and register this book’s practice tests using the registration code you just found. The process should take only a couple of minutes.

Customizing Your Exams

Once you are in the exam settings screen, you can choose to take exams in one of three modes:

- **Study mode:** Allows you to fully customize your exams and review answers as you are taking the exam. This is typically the mode you would use first to assess your knowledge and identify information gaps.
- **Practice Exam mode:** Locks certain customization options, as it is presenting a realistic exam experience. Use this mode when you are preparing to test your exam readiness.
- **Flash Card mode:** Strips out the answers and presents you with only the question stem. This mode is great for late-stage preparation when you really want to challenge yourself to provide answers without the benefit of seeing multiple-choice options. This mode does not provide the detailed score reports that the other two modes do, so you should not use it if you are trying to identify knowledge gaps.

In addition to these three modes, you will be able to select the source of your questions. You can choose to take exams that cover all of the chapters or you can narrow your selection to just a single chapter or the chapters that make up specific parts in the book. All chapters are selected by default. If you want to narrow your focus to individual chapters, simply deselect all the chapters and then select only those on which you wish to focus in the Objectives area.

You can also select the exam banks on which to focus. Each exam bank comes complete with a full exam of questions that cover topics in every chapter. The two exams printed in the book are available to you as well as two additional exams of unique questions. You can have the test engine serve up exams from all four banks or just from one individual bank by selecting the desired banks in the exam bank area.

There are several other customizations you can make to your exam from the exam settings screen, such as the time of the exam, the number of questions served up, whether to randomize questions and answers, whether to show the number of correct answers for multiple-answer questions, and whether to serve up only specific types of questions. You can also create custom test banks by selecting only questions that you have marked or questions on which you have added notes.

Updating Your Exams

If you are using the online version of the Pearson Test Prep software, you should always have access to the latest version of the software as well as the exam data. If you are using the Windows desktop version, every time you launch the software while connected to the Internet, it checks if there are any updates to your exam data and automatically downloads any changes that were made since the last time you used the software.

Sometimes, due to many factors, the exam data may not fully download when you activate your exam. If you find that figures or exhibits are missing, you may need to manually update your exams. To update a particular exam you have already activated and downloaded, simply click the **Tools** tab and click the **Update Products** button. Again, this is only an issue with the desktop Windows application.

If you wish to check for updates to the Pearson Test Prep exam engine software, Windows desktop version, simply click the **Tools** tab and click the **Update Application** button. This ensures that you are running the latest version of the software engine.

This page intentionally left blank

Software-Defined Networking Security and Network Programmability

This chapter covers the following topics:

- Software-Defined Networking (SDN) and SDN Security
- Network Programmability

This chapter starts with an introduction to SDN and different SDN security concepts, such as centralized policy management and micro-segmentation. This chapter also introduces SDN solutions such as Cisco ACI and modern networking environments such as Cisco DNA. You will also learn what network overlays are and what they are trying to solve.

The second part of this chapter provides an overview of network programmability and how networks are being managed using modern application programming interfaces (APIs) and other functions. This chapter also includes dozens of references that are available to enhance your learning.

The following SCOR 350-701 exam objectives are covered in this chapter:

- **Domain 1: Security Concepts**
 - 1.7 Explain northbound and southbound APIs in the SDN architecture
 - 1.8 Explain DNA Center (DNAC) APIs for network provisioning, optimization, monitoring, and troubleshooting

“Do I Know This Already?” Quiz

The “Do I Know This Already?” quiz allows you to assess whether you should read this entire chapter thoroughly or jump to the “Exam Preparation Tasks” section. If you are in doubt about your answers to these questions or your own assessment of your knowledge of the topics, read the entire chapter. Table 3-1 lists the major headings in this chapter and their corresponding “Do I Know This Already?” quiz questions. You can find the answers in Appendix A, “Answers to the ‘Do I Know This Already?’ Quizzes and Q&A Sections.”

Table 3-1 “Do I Know This Already?” Section-to-Question Mapping

| Foundation Topics Section | Questions |
|--|-----------|
| Software-Defined Networking (SDN) and SDN Security | 1–5 |
| Introduction to Network Programmability | 6–10 |

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

1. Which of the following are the three different “planes” in traditional networking?
 - a. The management, control, and data planes
 - b. The authorization, authentication, and accountability planes
 - c. The authentication, control, and data planes
 - d. None of these answers are correct.
2. Which of the following is true about Cisco ACI?
 - a. Spine nodes interconnect leaf devices, and they can also be used to establish connections from a Cisco ACI pod to an IP network or interconnect multiple Cisco ACI pods.
 - b. Leaf switches provide the Virtual Extensible LAN (VXLAN) tunnel endpoint (VTEP) function.
 - c. The APIC manages the distributed policy repository responsible for the definition and deployment of the policy-based configuration of the Cisco ACI infrastructure.
 - d. All of these answers are correct.
3. Which of the following is used to create network overlays?
 - a. SDN-Lane
 - b. VXLAN
 - c. VXWAN
 - d. None of these answers are correct.
4. Which of the following is an identifier or a tag that represents a logical segment?
 - a. VXLAN Network Identifier (VNID)
 - b. VXLAN Segment Identifier (VSID)
 - c. ACI Network Identifier (ANID)
 - d. Application Policy Infrastructure Controller (APIC)
5. Which of the following is network traffic between servers (virtual servers or physical servers), containers, and so on?
 - a. East-west traffic
 - b. North-south traffic
 - c. Micro-segmentation
 - d. Network overlays

6. Which of the following is an HTTP status code message range related to successful HTTP transactions?
 - a. Messages in the 100 range
 - b. Messages in the 200 range
 - c. Messages in the 400 range
 - d. Messages in the 500 range
7. Which of the following is a Python package that can be used to interact with REST APIs?
 - a. argparse
 - b. requests
 - c. rest_api_pkg
 - d. None of these answers are correct.
8. Which of the following is a type of API that exclusively uses XML?
 - a. APIC
 - b. REST
 - c. SOAP
 - d. GraphQL
9. Which of the following is a modern framework of API documentation and is now the basis of the OpenAPI Specification (OAS)?
 - a. SOAP
 - b. REST
 - c. Swagger
 - d. WSDL
10. Which of the following can be used to retrieve a network device configuration?
 - a. RESTCONF
 - b. NETCONF
 - c. SNMP
 - d. All of these answers are correct.

Foundation Topics

Software-Defined Networking (SDN) and SDN Security

In the last decade there have been several shifts in networking technologies. Some of these changes are due to the demand of modern applications in very diverse environments and the cloud. This complexity introduces risks, including network configuration errors that can cause significant downtime and network security challenges.

Subsequently, networking functions such as routing, optimization, and security have also changed. The next generation of hardware and software components in enterprise networks must support both the rapid introduction and the rapid evolution of new technologies and solutions. Network infrastructure solutions must keep pace with the business environment and support modern capabilities that help drive simplification within the network.

These elements have fueled the creation of software-defined networking (SDN). SDN was originally created to decouple control from the forwarding functions in networking equipment. This is done to use software to centrally manage and “program” the hardware and virtual networking appliances to perform forwarding.



Traditional Networking Planes

In traditional networking, there are three different “planes” or elements that allow network devices to operate: the management, control, and data planes. Figure 3-1 shows a high-level explanation of each of the planes in traditional networking.

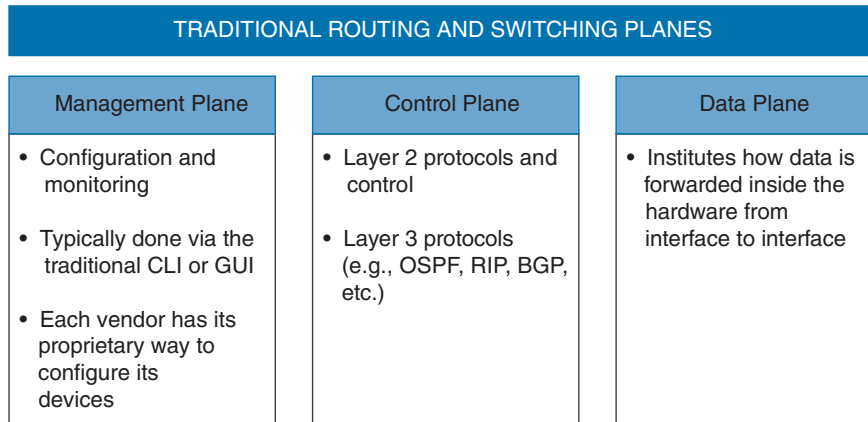


Figure 3-1 *The Management, Control, and Data Planes*

The control plane has always been separated from the data plane. There was no central brain (or controller) that controlled the configuration and forwarding. Let’s take a look at the example shown in Figure 3-2. Routers, switches, and firewalls were managed by the command-line interface (CLI), graphical user interfaces (GUIs), and custom Tcl scripts. For instance, the firewalls were managed by the Adaptive Security Device Manager (ASDM), while the routers were managed by the CLI.

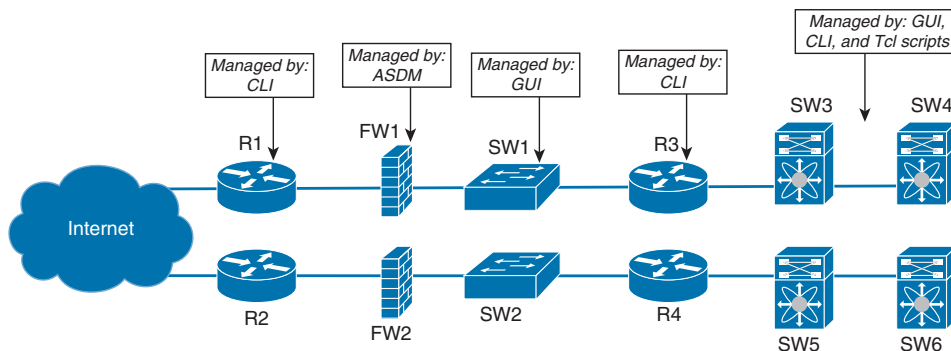


Figure 3-2 *Traditional Network Management Solutions*

Each device in Figure 3-2 has its “own brain” and does not really exchange any intelligent information with the rest of the devices.

**Key
Topic****So What's Different with SDN?**

SDN introduced the notion of a centralized controller. The SDN controller has a global view of the network, and it uses a common management protocol to configure the network infrastructure devices. The SDN controller can also calculate reachability information from many systems in the network and pushes a set of flows inside the switches. The flows are used by the hardware to do the forwarding. Here you can see a clear transition from a distributed “semi-intelligent brain” approach to a “central and intelligent brain” approach.

TIP An example of an open-source implementation of SDN controllers is the Open vSwitch (OVS) project using the OVS Database (OVSDB) management protocol and the OpenFlow protocol. Another example is the Cisco Application Policy Infrastructure Controller (Cisco APIC). Cisco APIC is the main architectural component and the brain of the Cisco Application Centric Infrastructure (ACI) solution. A great example of this is Cisco ACI, which is discussed in the next section of the chapter.

SDN changed a few things in the management, control, and data planes. However, the big change was in the control and data planes in software-based switches and routers (including virtual switches inside of hypervisors). For instance, the Open vSwitch project started some of these changes across the industry.

SDN provides numerous benefits in the management plane. These benefits are in both physical switches and virtual switches. SDN is now widely adopted in data centers. A great example of this is Cisco ACI.

**Key
Topic****Introduction to the Cisco ACI Solution**

Cisco ACI provides the ability to automate setting networking policies and configurations in a very flexible and scalable way. Figure 3-3 illustrates the concept of a centralized policy and configuration management in the Cisco ACI solution.

The Cisco ACI scenario shown in Figure 3-3 uses a leaf-and-spine topology. Each leaf switch is connected to every spine switch in the network with no interconnection between leaf switches or spine switches.

The leaf switches have ports connected to traditional Ethernet devices (for example, servers, firewalls, routers, and so on). Leaf switches are typically deployed at the edge of the fabric. These leaf switches provide the Virtual Extensible LAN (VXLAN) tunnel endpoint (VTEP) function. VXLAN is a network virtualization technology that leverages an encapsulation technique (similar to VLANs) to encapsulate Layer 2 Ethernet frames within UDP packets (over UDP port 4789, by default).

NOTE The section “VXLAN and Network Overlays,” later in the chapter, will discuss VXLAN and overlays in more detail.

In Cisco ACI, the IP address that represents the leaf VTEP is called the physical tunnel endpoint (PTEP). The leaf switches are responsible for routing or bridging tenant packets and for applying network policies.

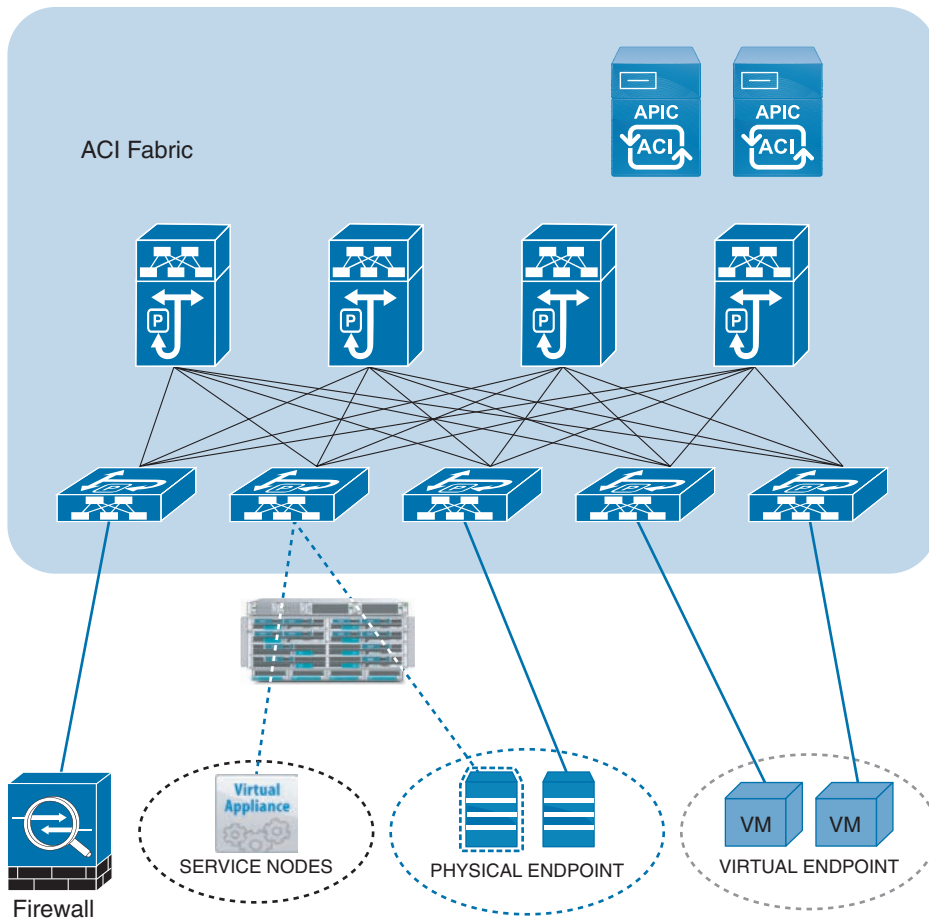


Figure 3-3 Cisco APIC Configuration and Policy Management

Spine nodes interconnect leaf devices, and they can also be used to establish connections from a Cisco ACI pod to an IP network or to interconnect multiple Cisco ACI pods. Spine switches store all the endpoint-to-VTEP mapping entries. All leaf nodes connect to all spine nodes within a Cisco ACI pod. However, no direct connectivity is allowed between spine nodes or between leaf nodes.

NOTE All workloads in Cisco ACI connect to leaf switches. The leaf switches used in a Cisco ACI fabric are Top-of-the-Rack (ToR) switches. The acronym “ToR” here is not the same as “The Onion Router” (a solution used for anonymity and to access the “deep web”).

The APIC can be considered a policy and a topology manager. APIC manages the distributed policy repository responsible for the definition and deployment of the policy-based configuration of the Cisco ACI infrastructure. APIC also manages the topology and inventory information of all devices within the Cisco ACI pod.

**Key
Topic**

The following are additional functions of the APIC:

- The APIC “observer” function monitors the health, state, and performance information of the Cisco ACI pod.
- The “boot director” function is in charge of the booting process and firmware updates of the spine switches, leaf switches, and the APIC components.
- The “appliance director” APIC function manages the formation and control of the APIC appliance cluster.
- The “virtual machine manager (VMM)” is an agent between the policy repository and a hypervisor. The VMM interacts with hypervisor management systems (for example, VMware vCenter).
- The “event manager” manages and stores all the events and faults initiated from the APIC and the Cisco ACI fabric nodes.
- The “appliance element” maintains the inventory and state of the local APIC appliance.

TIP The Cisco ACI Design Guide provides comprehensive information about the design, deployment, and configuration of the ACI solution. The design guide can be found here: <https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-737909.pdf>.

**Key
Topic**

VXLAN and Network Overlays

Modern networks and data centers need to provide load balancing, better scalability, elasticity, and faster convergence. Many organizations use the overlay network model. Deploying an overlay network allows you to tunnel Layer 2 Ethernet packets with different encapsulations over a Layer 3 network. The overlay network uses “tunnels” to carry the traffic across the Layer 3 fabric. This solution also needs to allow the “underlay” to separate network flows between different “tenants” (administrative domains). The solution also needs to switch packets within the same Layer 2 broadcast domain, route traffic between Layer 3 broadcast domains, and provide IP separation, traditionally done via virtual routing and forwarding (VRF).

There have been multiple IP tunneling mechanisms introduced throughout the years. The following are a few examples of tunneling mechanisms:

- Virtual Extensible LAN (VXLAN)
- Network Virtualization using Generic Routing Encapsulation (NVGRE)
- Stateless Transport Tunneling (STT)
- Generic Network Virtualization Encapsulation (GENEVE)

All of the aforementioned tunneling protocols carry an Ethernet frame inside an IP frame. The main difference between them is in the type of the IP frame used. For instance, VXLAN uses UDP, and STT uses TCP.

The use of UDP in VXLAN enables routers to apply hashing algorithms on the outer UDP header to load balance network traffic. Network traffic that is riding the overlay network tunnels is load balanced over multiple links using equal-cost multi-path routing (ECMP). This introduces a better solution compared to traditional network designs. In traditional network designs, access switches connect to distribution switches. This causes redundant links to block due to spanning tree.

VXLAN uses an identifier or a tag that represents a logical segment that is called the VXLAN Network Identifier (VNID). The logical segment identified with the VNID is a Layer 2 broadcast domain that is tunneled over the VTEP tunnels.

Figure 3-4 shows an example of an overlay network that provides Layer 2 capabilities.

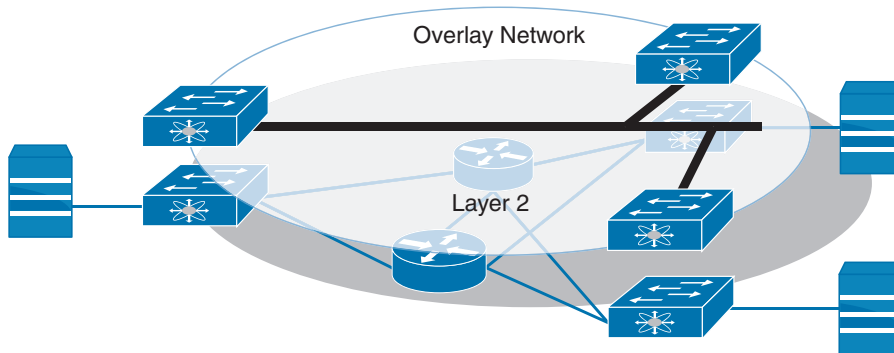


Figure 3-4 *Overlay Network Providing Layer 2 Capabilities*

Figure 3-5 shows an example of an overlay network that provides Layer 3 routing capabilities.

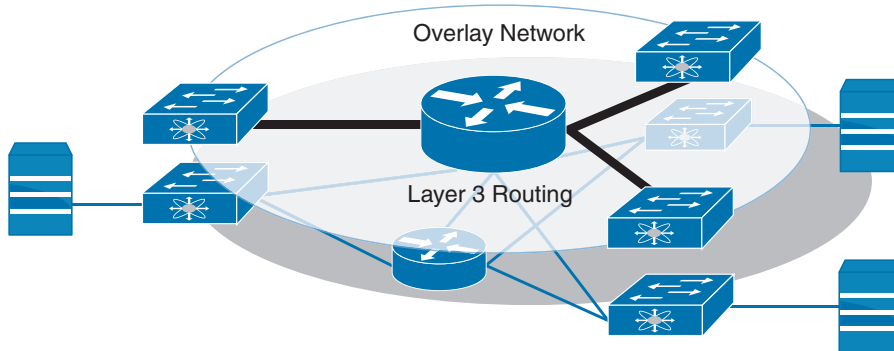


Figure 3-5 *Overlay Network Providing Layer 3 Routing Capabilities*

Figure 3-6 illustrates the VXLAN frame format for your reference.

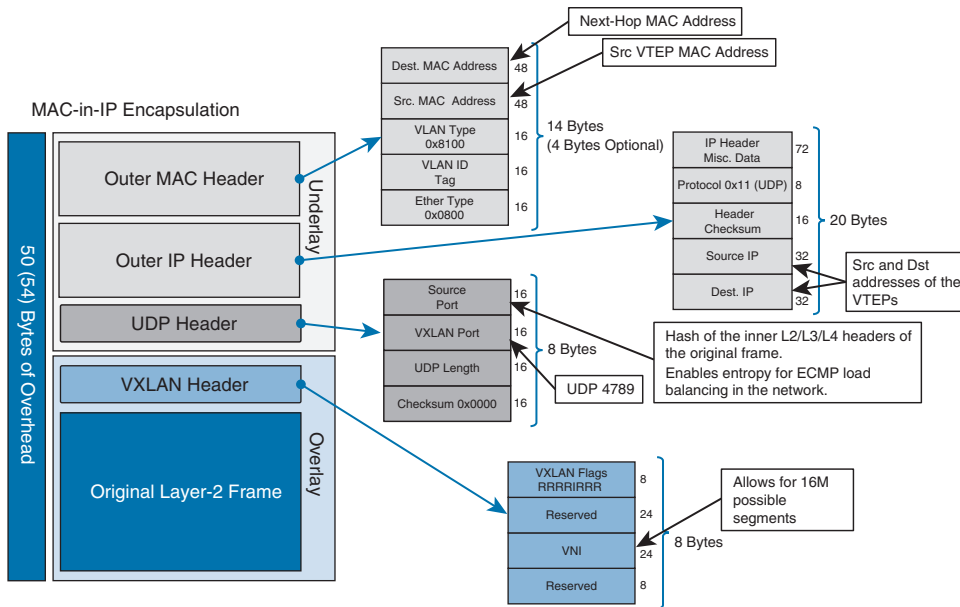


Figure 3-6 VXLAN Frame Format

Micro-Segmentation

Key Topic

For decades, servers were assigned subnets and VLANs. Sounds pretty simple, right? Well, this introduced a lot of complexities because application segmentation and policies were physically restricted to the boundaries of the VLAN within the same data center (or even in “the campus”). In virtual environments, the problem became harder. Nowadays applications can move around between servers to balance loads for performance or high availability upon failures. They also can move between different data centers and even different cloud environments.

Traditional segmentation based on VLANs constrains you to maintain the policies of which application needs to talk to which application (and who can access such applications) in centralized firewalls. This is ineffective because most traffic in data centers is now “East-West” traffic. A lot of that traffic does not even hit the traditional firewall. In virtual environments, a lot of the traffic does not even leave the physical server.

Key Topic

Let’s define what people refer to as “East-West” traffic and “North-South” traffic. “East-West” traffic is network traffic between servers (virtual servers or physical servers, containers, and so on).

“North-South” traffic is network traffic flowing in and outside the data center. Figure 3-7 illustrates the concepts of “East-West” and “North-South” traffic.

Many vendors have created solutions where policies applied to applications are independent from the location or the network tied to the application.

For example, let’s suppose that you have different applications running in separate VMs and those applications also need to talk to a database (as shown in Figure 3-8).

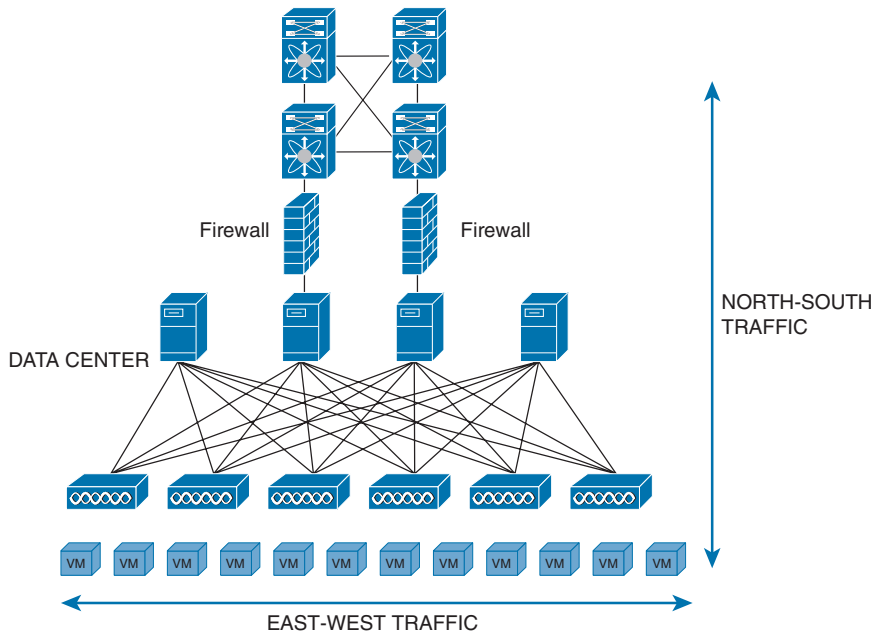


Figure 3-7 “East-West” and “North-South” Traffic

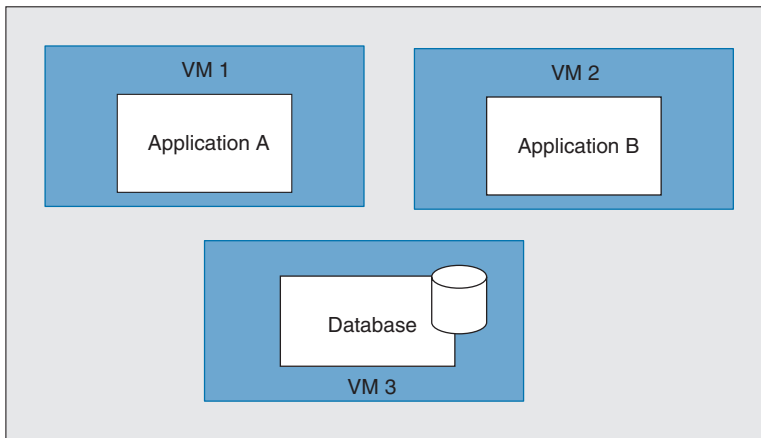


Figure 3-8 Applications in VMs

You need to apply policies to restrict if application A needs or does not need to talk to application B, or which application should be able to talk to the database. These policies should not be bound by which VLAN or IP subnet the application belongs to and whether it is in the same rack or even in the same data center. Network traffic should not make multiple trips back and forth between the applications and centralized firewalls to enforce policies between VMs.

Containers make this a little harder because they move and change more often. Figure 3-9 illustrates a high-level representation of applications running inside of containers (for example, Docker containers).

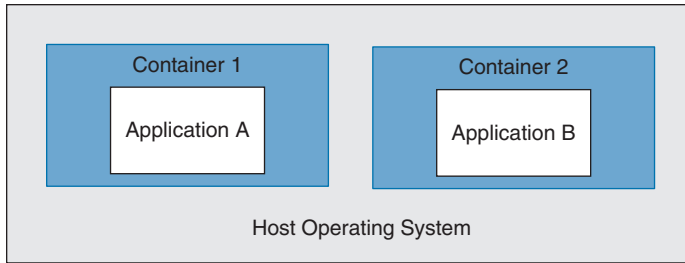


Figure 3-9 *Applications in Containers*

The ability to enforce network segmentation in those environments is called “micro-segmentation.” Micro-segmentation is at the VM level or between containers regardless of a VLAN or a subnet. Micro-segmentation solutions need to be “application aware.” This means that the segmentation process starts and ends with the application itself.

Most micro-segmentation environments apply a “zero-trust model.” This model dictates that users cannot talk to applications, and applications cannot talk to other applications unless a defined set of policies permits them to do so.

**Key
Topic**

Open-Source Initiatives

Several open-source projects are trying to provide micro-segmentation and other modern networking benefits. Examples include the following:

- Neutron from OpenStack
- Open vSwitch (OVS)
- Open Virtual Network (OVN)
- OpenDaylight (ODL)
- Open Platform for Network Function Virtualization (OPNFV)
- Contiv

The concept of SDN is very broad, and every open-source provider and commercial vendor takes it in a different direction. The networking component of OpenStack is called Neutron. Neutron is designed to provide “networking as a service” in private, public, and hybrid cloud environments. Other OpenStack components, such as Horizon (Web UI) and Nova (compute service), interact with Neutron using a set of APIs to configure the networking services. Neutron uses plug-ins to deliver advanced networking capabilities and allow third-party vendor integration. Neutron has two main components: the neutron server and a database that handles persistent storage and plug-ins to provide additional services. Additional information about Neutron and OpenStack can be found at <https://docs.openstack.org/neutron/latest>.

OVN was originally created by the folks behind Open vSwitch (OVS) for the purpose of bringing an open-source solution for virtual network environments and SDN. Open vSwitch is an open-source implementation of a multilayer virtual switch inside the hypervisor.

NOTE You can download Open vSwitch and access its documentation at <https://www.openvswitch.org>.

OVN is often used in OpenStack implementations with the use of OVS. You can also use OVN with the OpenFlow protocol. OpenStack Neutron uses OVS as the default “control plane.”

NOTE You can access different tutorials about OVN and OVS at <http://docs.openvswitch.org/en/latest/tutorials/>.

OpenDaylight (ODL) is another popular open-source project that is focused on the enhancement of SDN controllers to provide network services across multiple vendors. OpenDaylight participants also interact with the OpenStack Neutron project and attempt to solve the existing inefficiencies.

OpenDaylight interacts with Neutron via a northbound interface and manages multiple interfaces southbound, including the Open vSwitch Database Management Protocol (OVSDB) and OpenFlow.

TIP You can find more information about OpenDaylight at <https://www.opendaylight.org>. Cisco has several tutorials and additional information about OpenDaylight in DevNet at <https://developer.cisco.com/site/opendaylight/>.

Key Topic

So, what is a northbound and southbound API? In an SDN architecture, southbound APIs are used to communicate between the SDN controller and the switches and routers within the infrastructure. These APIs can be open or proprietary.

NOTE Cisco provides detailed information about the APIs supported in all platforms in DevNet (developer.cisco.com). DevNet will be discussed in detail later in this chapter.

Southbound APIs enable SDN controllers to dynamically make changes based on real-time demands and scalability needs. OpenFlow and Cisco OpFlex provide southbound API capabilities.

Northbound APIs (SDN northbound APIs) are typically RESTful APIs that are used to communicate between the SDN controller and the services and applications running over the network. Such northbound APIs can be used for the orchestration and automation of the network components to align with the needs of different applications via SDN network programmability. In short, northbound APIs are basically the link between the applications and the SDN controller. In modern environments, applications can tell the network devices (physical or virtual) what type of resources they need and, in turn, the SDN solution can provide the necessary resources to the application.

Cisco has the concept of intent-based networking. On different occasions, you may see northbound APIs referred to as “intent-based APIs.”

Key Topic

More About Network Function Virtualization

Network virtualization is used for logical groupings of nodes on a network. The nodes are abstracted from their physical locations so that VMs and any other assets can be managed as if they are all on the same physical segment of the network. This is not a new technology.

However, it is still one that is key in virtual environments where systems are created and moved despite their physical location.

Network Functions Virtualization (NFV) is a technology that addresses the virtualization of Layer 4 through Layer 7 services. These include load balancing and security capabilities such as firewall-related features. In short, with NFV, you convert certain types of network appliances into VMs. NFV was created to address the inefficiencies that were introduced by virtualization.

NFV allows you to create a virtual instance of a virtual node such as a firewall that can be deployed where it is needed, in a flexible way that's similar to what you do with a traditional VM.

Open Platform for Network Function Virtualization (OPNFV) is an open-source solution for NFV services. It aims to be the base infrastructure layer for running virtual network functions. You can find detailed information about OPNFV at opnfv.org.

NFV nodes such as virtual routers and firewalls need an underlying infrastructure:

- A hypervisor to separate the virtual routers, switches, and firewalls from the underlying physical hardware. The hypervisor is the underlying virtualization platform that allows the physical server (system) to operate multiple VMs (including traditional VMs and network-based VMs).
- A virtual forwarder to connect individual instances.
- A network controller to control all of the virtual forwarders in the physical network.
- A VM manager to manage the different network-based VMs.

Figure 3-10 demonstrates the high-level components of the NFV architecture.

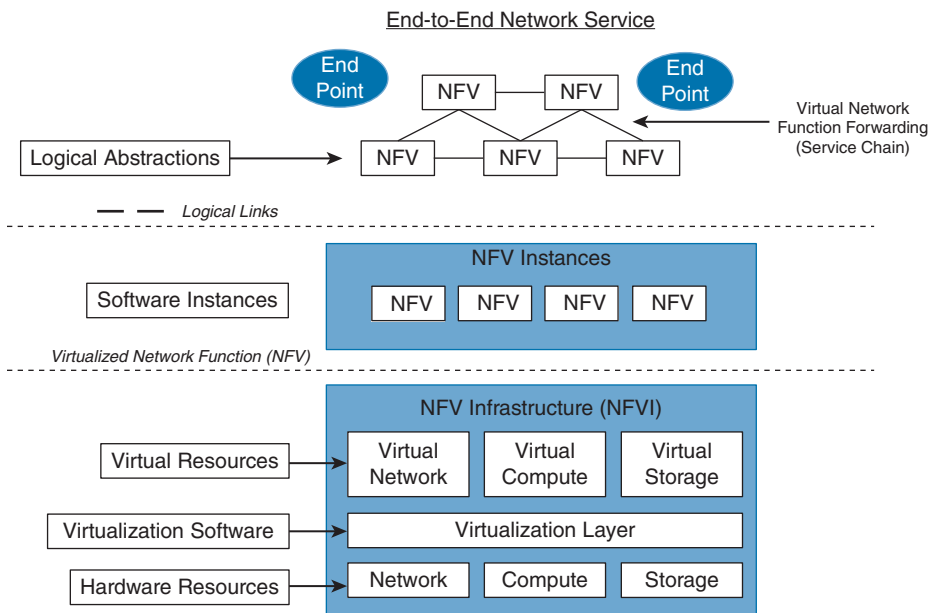


Figure 3-10 NFV Architecture

Several NFV infrastructure components have been created in open community efforts. On the other hand, traditionally, the actual integration has so far remained a “private” task. You’ve either had to do it yourself, outsource it, or buy a pre-integrated system from some vendor, keeping in mind that the systems integration undertaken is not a one-time task. OPNFV was created to change the NFV ongoing integration task from a private solution into an open community solution.

NFV MANO

NFV changes the way networks are managed. NFV management and network orchestration (MANO) is a framework and working group within the European Telecommunications Standards Institute (ETSI) Industry Specification Group for NFV (ETSI ISG NFV). NFV MANO is designed to provide flexible onboarding of network components. NFV MANO is divided into the three functional components listed in Figure 3-11.

| NFV Orchestrator | VNF Manager | Virtualized Infrastructure Manager (VIM) |
|--|--|--|
| <ul style="list-style-type: none"> Onboards (orchestrates) new network services (NS) and virtual network function (VNF) packages. The NFV Orchestrator is also responsible for the lifecycle management; global resource management; validation and authorization of network functions virtualization infrastructure (NFVI) resource requests. | <ul style="list-style-type: none"> Oversees lifecycle management of VNF instances. Coordinates configuration and event reporting between NFV infrastructure (NFVI) and Element/Network Management Systems. | <ul style="list-style-type: none"> Controls and manages the NFVI compute, storage, and network resources. |

Figure 3-11 NFV MANO Functional Components

The NFV MANO architecture is integrated with open application program interfaces (APIs) in the existing systems. The MANO layer works with templates for standard VNFs. It allows implementers to pick and choose from existing NFV resources to deploy their platform or element.

Contiv

Contiv is an open-source project that allows you to deploy micro-segmentation policy-based services in container environments. It offers a higher level of networking abstraction for microservices by providing a policy framework. Contiv has built-in service discovery and service routing functions to allow you to scale out services.

NOTE You can download Contiv and access its documentation at <https://contiv.io>.

With Contiv you can assign an IP address to each container. This feature eliminates the need for host-based port NAT. Contiv can operate in different network environments such as traditional Layer 2 and Layer 3 networks, as well as overlay networks.

Contiv can be deployed with all major container orchestration platforms (or schedulers) such as Kubernetes and Docker Swarm. For instance, Kubernetes can provide compute resources to containers and then Contiv provides networking capabilities.

NOTE Contiv supports Layer 2, Layer 3 (BGP), VXLAN for overlay networks, and Cisco ACI mode. It also provides built-in east-west service load balancing and traffic isolation.

The Netmaster and Netplugin (Contiv host agent) are the two major components in Contiv. Figure 3-12 illustrates how the Netmaster and the Netplugin interact with all the underlying components of the Contiv solution.

TIP The Contiv website includes several tutorials and step-by-step integration documentation at <https://contiv.io/documents/tutorials/index.html>.

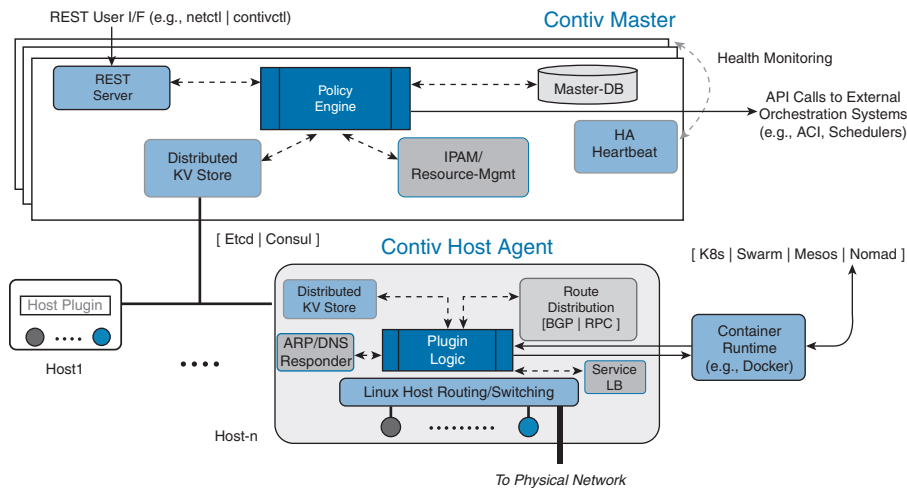


Figure 3-12 Contiv Netmaster and Netplugin (Contiv Host Agent) Components

ThousandEyes Integration

ThousandEyes, the leading network intelligence Software as a Service (SaaS) platform, has taken its partnership with Cisco to the next level. The integration of ThousandEyes into the Cisco Nexus 9000 Series data center switches, powered by NX-OS/Data Center Network Manager (DCNM), and its integration into Cisco ACI fabrics, delivers a powerful combination of network visibility and control.

With the Cisco ThousandEyes Enterprise Agent (TEA), users can now monitor their network's performance from a global perspective, utilizing a range of tests to assess BGP routing, DNS resolution, browser response times, network pathing and connectivity, routing status, and VoIP streaming quality. This integration offers unparalleled insight and control to help organizations optimize their network performance. ThousandEyes provides numerous monitoring capabilities including the following:

- API Monitoring
- BGP Monitoring
- CDN Monitoring

- Customer Digital Experience
- DDoS Monitoring
- DNS Monitoring
- Enterprise Digital Experience
- Hybrid WAN Monitoring
- Network Device Monitoring
- Network Monitoring
- IaaS Monitoring
- ISP Monitoring
- Multi-cloud Monitoring
- SaaS Monitoring
- SD-WAN Monitoring
- VPN Monitoring
- Website Monitoring
- Wi-Fi and LAN Monitoring

Cisco Digital Network Architecture (DNA)

Cisco DNA is a solution created by Cisco that is often referred to as the “intent-based networking” solution. Cisco DNA provides automation and assurance services across campus networks, wide area networks (WANs), and branch networks. Cisco DNA is based on an open and extensible platform and provides the policy, automation, and analytics capabilities, as illustrated in Figure 3-13.

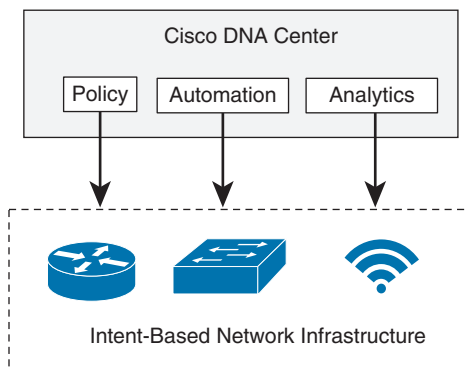


Figure 3-13 Cisco DNA High-Level Architecture

The heart of the Cisco DNA solution is Cisco DNA Center (DNAC). DNAC is a command-and-control element that provides centralized management via dashboards and APIs. Figure 3-14 shows one of the many dashboards of Cisco DNA Center (the Network Hierarchy dashboard).

Cisco DNA Center can be integrated with external network and security services such as the Cisco Identity Services Engine (ISE). Figure 3-15 shows how the Cisco ISE is configured as an authentication, authorization, and accounting (AAA) server in the Cisco DNA Center Network Settings screen.

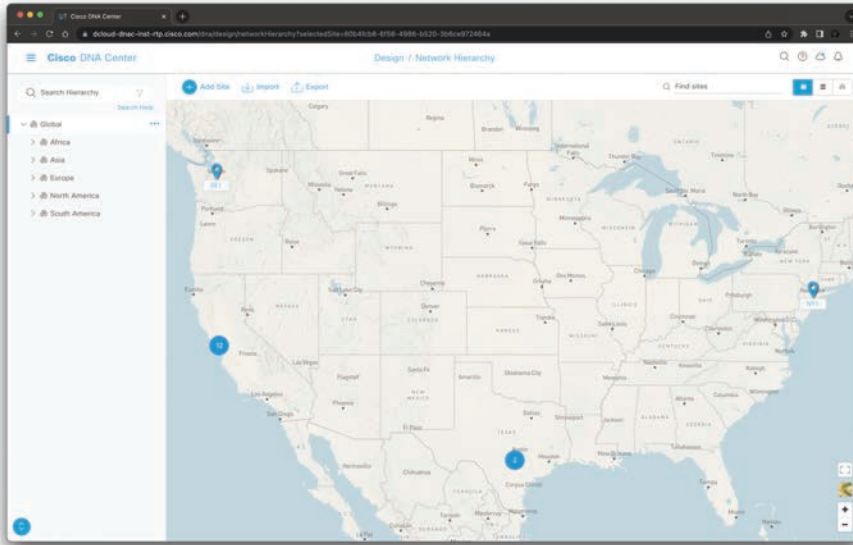


Figure 3-14 Cisco DNA Center Network Hierarchy Dashboard

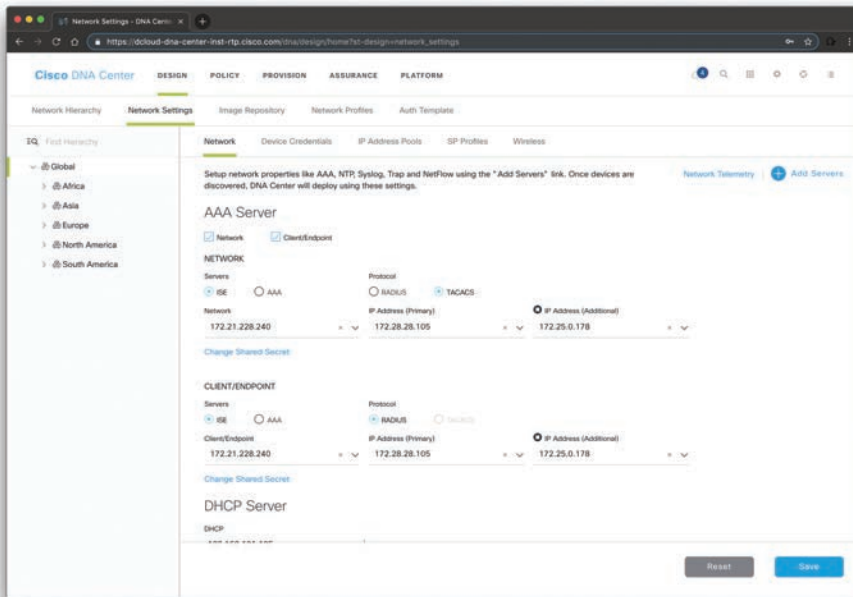


Figure 3-15 Cisco DNA Center Integration with Cisco ISE for AAA Services

Cisco DNA Policies

The following are the policies you can create in the Cisco DNA Center:

- Group-based access control policies
- IP-based access control policies
- Application access control policies
- Traffic copy policies

Figure 3-16 shows the Cisco DNA Center Policy Overview dashboard matrix visualization. Here, you can see the number of active policies based on the security groups, Cisco Identity Services Engine (ISE) profiles, and Cisco Secure Network Analytics (formerly known as Stealthwatch) host groups. Using the dashboard shown in Figure 3-16, you can create new policies.

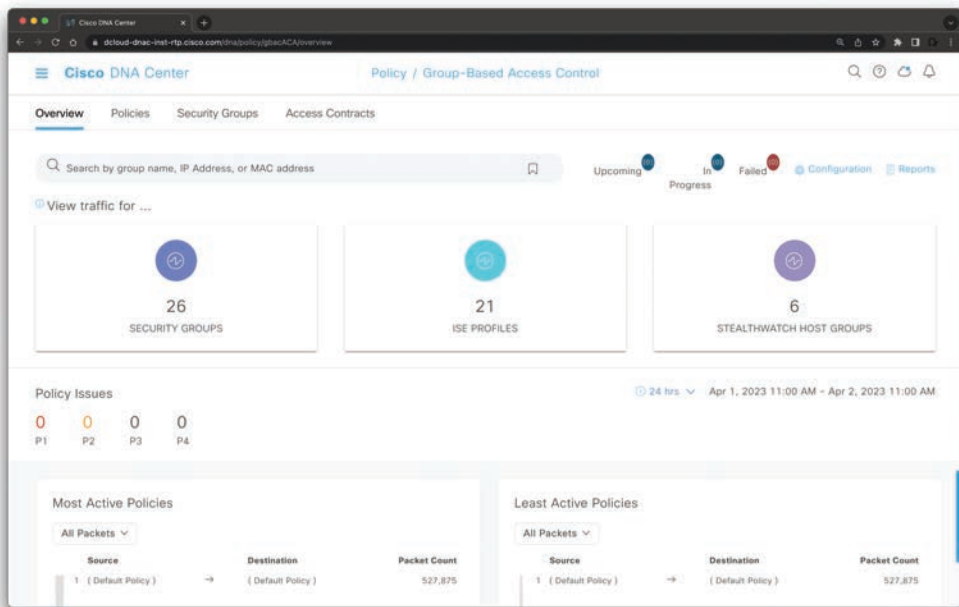


Figure 3-16 Cisco DNA Center Policy Overview Dashboard

Figure 3-17 shows the policy analytics for the ISE profiles. Cisco DNA Center empowers you with intelligence and analytics to make informed decisions about your network. With its visual representation of communication between assets, you can easily create group-based policies, evaluate the effects of new access controls, and determine the precise protocols that should be included in your policies. This comprehensive solution provides you with a clear understanding of your network, enabling you to take control and optimize its performance.

Figure 3-18 shows the policy matrix. The matrix view enables you to have a comprehensive overview of all the source and destination policies and grasp the overall policy structure. You can view, create, and modify access control policies from the policy matrix view itself.

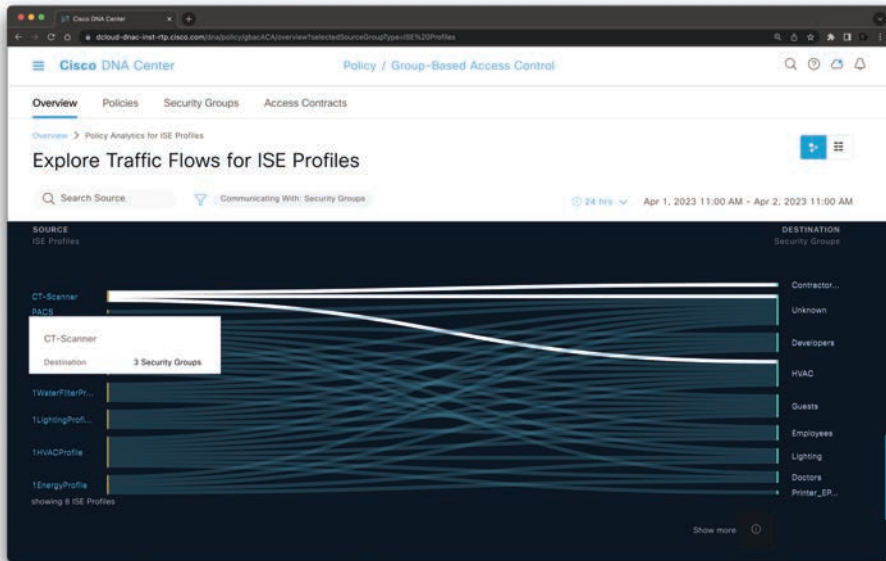


Figure 3-17 Policy Analytics for the ISE Profiles in DNA Center

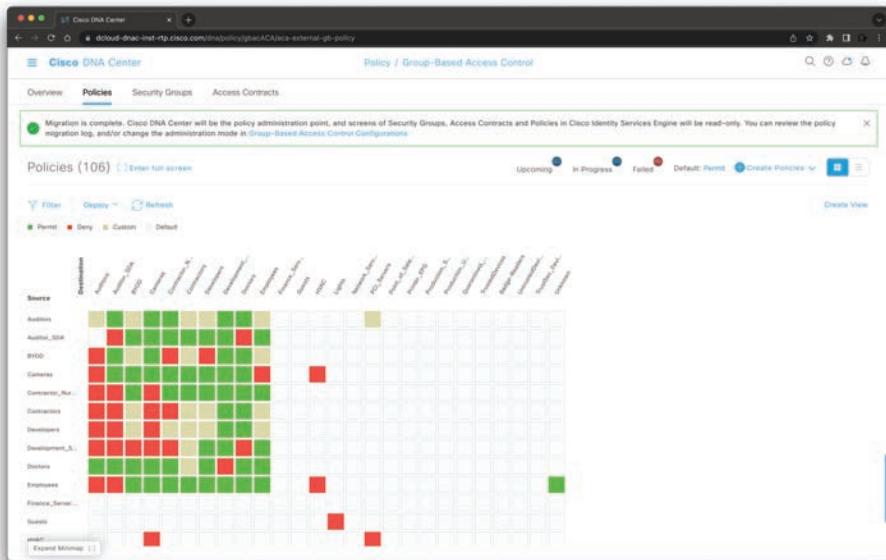


Figure 3-18 DNA Center Policy Matrix

The matrix view has two components:

- **Source axis:** The vertical axis displays a list of all the source security groups.
- **Destination axis:** The horizontal axis presents a list of all the destination security groups.

By hovering over a cell, you can view the policy for a specific combination of source and destination security groups. The color of a cell represents the policy that is in effect, with the following color coding:

- **Allow:** Green
- **Block:** Red
- **Custom:** Gold
- **Default:** Gray

Cisco DNA Group-Based Access Control Policy

When you configure group-based access control policies, you need to integrate the Cisco ISE with Cisco DNA Center, as you learned previously in this chapter. In Cisco ISE, you configure the work process setting as “Single Matrix” so that there is only one policy matrix for all devices in the TrustSec network. You will learn more about Cisco TrustSec and Cisco ISE in Chapter 4, “Authentication, Authorization, Accounting (AAA) and Identity Management.”

Depending on your organization’s environment and access requirements, you can segregate your groups into different virtual networks to provide further segmentation.

After Cisco ISE is integrated in Cisco DNA Center, the scalable groups that exist in Cisco ISE are propagated to Cisco DNA Center. If a scalable group that you need does not exist, you can create it in Cisco ISE.

NOTE You can access Cisco ISE through the Cisco DNA Center interface to create scalable groups. After you have added a scalable group in Cisco ISE, it is synchronized with the Cisco DNA Center database so that you can use it in an access control policy. You cannot edit or delete scalable groups from Cisco DNA Center; you need to perform these tasks from Cisco ISE.

Cisco DNA Center has the concept of access control contracts. A contract specifies a set of rules that allow or deny network traffic based on such traffic matching particular protocols or ports. Figure 3-19 shows a new contract being created in Cisco DNA Center to allow SSH access (TCP port 22).

To create a contract, navigate to **Policy > Group-Based Access Control > Access Contract** and click **Add Contract**. The dialog box shown in Figure 3-19 will be displayed.

Figure 3-20 shows an example of how to create a group-based access control policy.

In Figure 3-20, an access control policy named **omar_policy_1** is configured to **deny** traffic from all users and related devices in the group called **Guests** to any user or device in the **Finance** group.

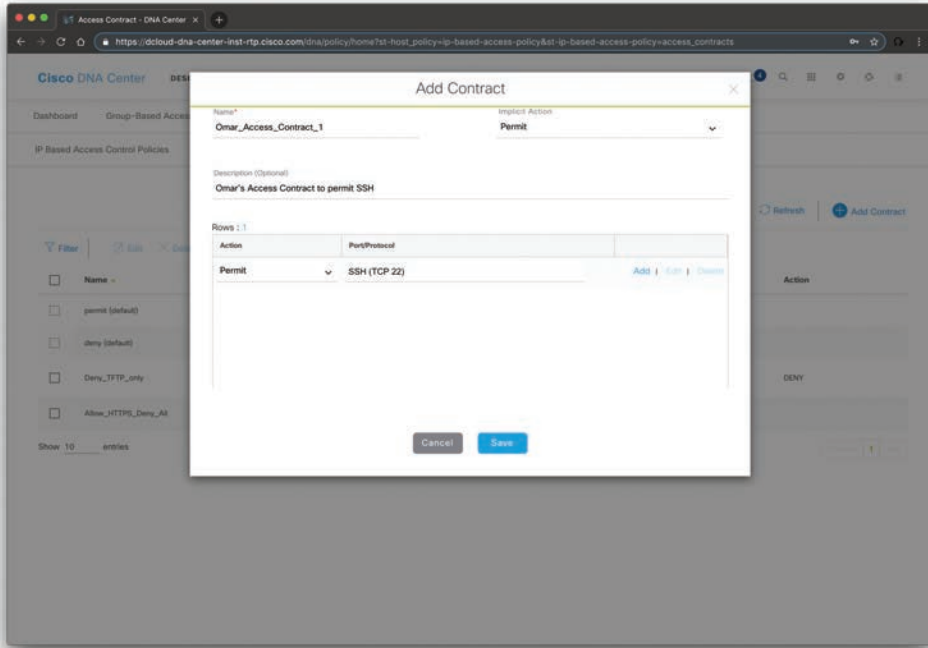


Figure 3-19 Adding a Cisco DNA Center Contract

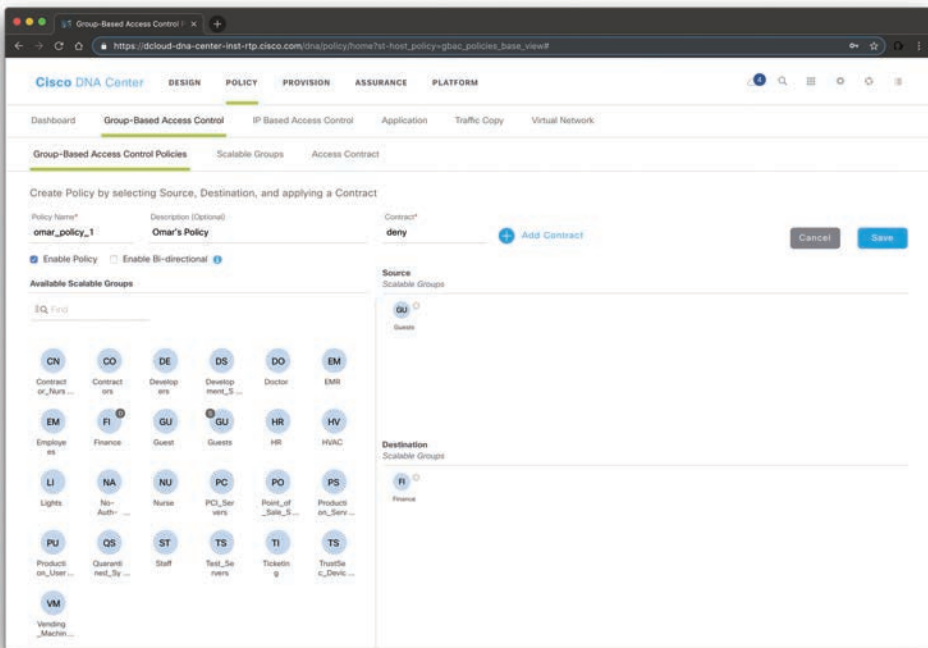


Figure 3-20 Adding a Cisco DNA Center Group-Based Access Control Policy

Cisco DNA IP-Based Access Control Policy

You can also create IP-based access control policies in Cisco DNA Center. To create IP-based access control policies, navigate to **Policy > IP Based Access Control > IP Based Access Control Policies**, as shown in Figure 3-21.

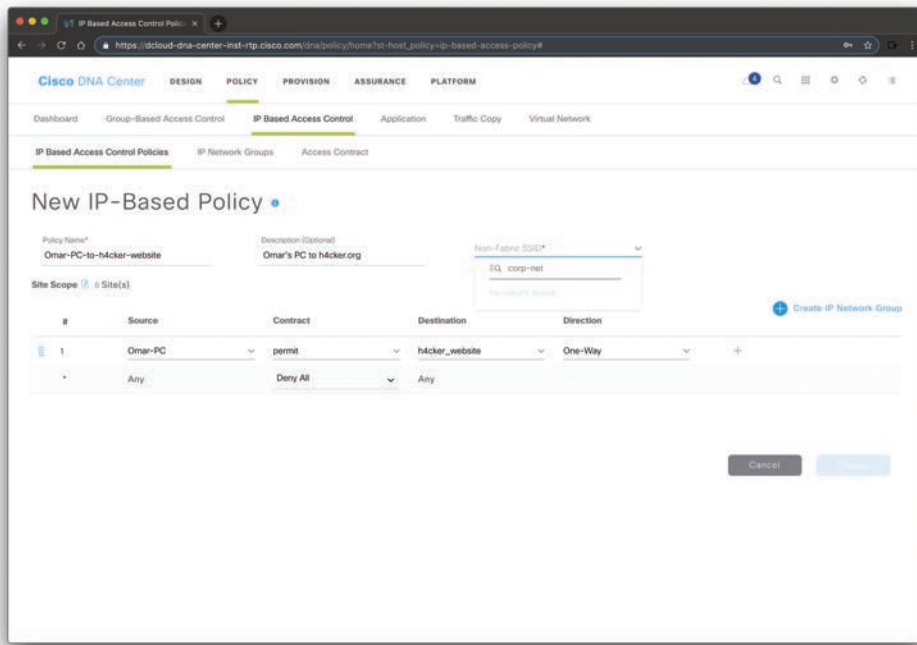


Figure 3-21 Adding a Cisco DNA Center IP-Based Access Control Policy

In the example shown in Figure 3-21, a policy is configured to permit Omar's PC to communicate with h4cker.org.

NOTE An IP network group named h4cker_website is already configured. To configure IP network groups, navigate to **Policy > IP Based Access Control > IP Network Groups**. These IP network groups can also be automatically populated from Cisco ISE.

You can also associate these policies to specific wireless SSIDs. The **corp-net** SSID is associated to the policy entry in Figure 3-21.

Cisco DNA Application Policies

Application policies can be configured in Cisco DNA Center to provide Quality of Service (QoS) capabilities. The following are the Application Policy components you can configure in Cisco DNA Center:

- Applications
- Application sets

- Application policies
- Queuing profiles

Applications in Cisco DNA Center are the software programs or network signaling protocols that are being used in your network.

NOTE Cisco DNA Center supports all of the applications in the Cisco Next Generation Network-Based Application Recognition (NBAR2) library.

Applications can be grouped into logical groups called *application sets*. These application sets can be assigned a business relevance within a policy.

You can also map applications to industry standard-based traffic classes, as defined in RFC 4594.

Cisco DNA Traffic Copy Policy

You can also use an Encapsulated Remote Switched Port Analyzer (ERSPAN) configuration in Cisco DNA Center so that the IP traffic flow between two entities is copied to a given destination for monitoring or troubleshooting. In order for you to configure ERSPAN using Cisco DNA Center, you need to create a traffic copy policy that defines the source and destination of the traffic flow you want to copy. To configure a traffic copy policy, navigate to **Policy > Traffic Copy > Traffic Copy Policies**, as shown in Figure 3-22.

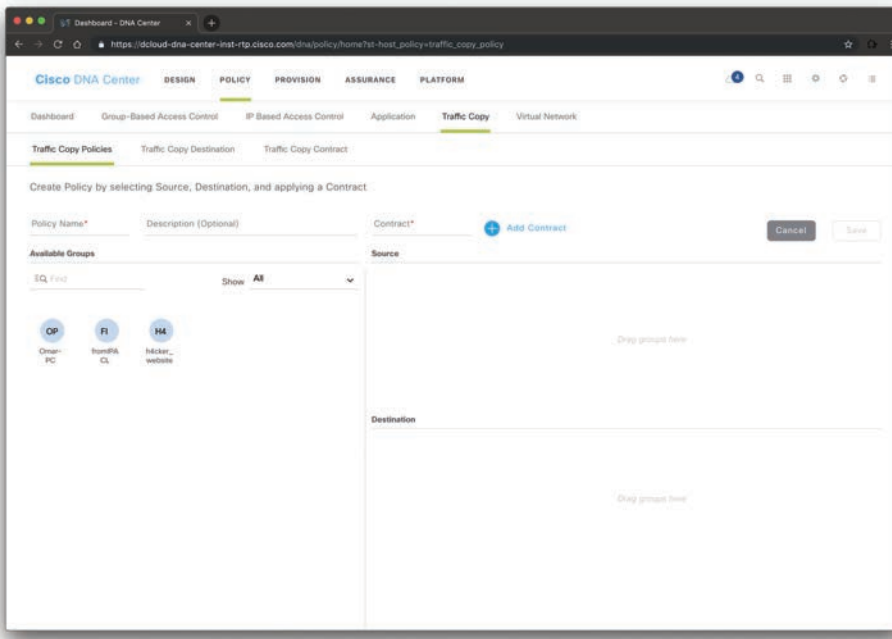


Figure 3-22 Adding a Traffic Copy Policy

You can also define a traffic copy contract that specifies the device and interface where the copy of the traffic is sent.

Cisco DNA Center Assurance Solution

The Cisco DNA Center Assurance solution allows you to get contextual visibility into network functions with historical, real-time, and predictive insights across users, devices, applications, and the network. The goal is to provide automation capabilities to reduce the time spent on network troubleshooting.

Figure 3-23 shows the Cisco DNA Center Assurance Overall Health dashboard.

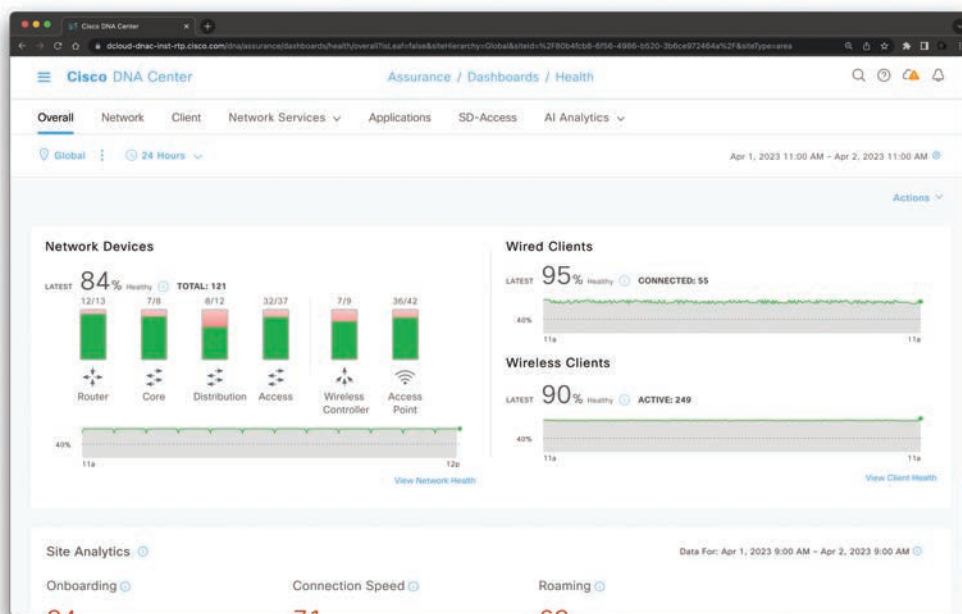


Figure 3-23 The Cisco DNA Center Assurance Overall Health Dashboard

The Cisco DNA Center Assurance solution allows you to investigate different networkwide (global) issues, as shown in Figure 3-24.

The Cisco DNA Center Assurance solution also allows you to configure sensors to test the health of wireless networks. A wireless network includes access point (AP) radios, WLAN configurations, and wireless network services. Sensors can be dedicated or on-demand sensors. A dedicated sensor is when an AP is converted into a sensor, and it stays in sensor mode (is not used by wireless clients) unless it is manually converted back into AP mode. An on-demand sensor is when an AP is temporarily converted into a sensor to run tests. After the tests are complete, the sensor goes back to AP mode. Figure 3-25 shows statistics about wired and wireless clients.

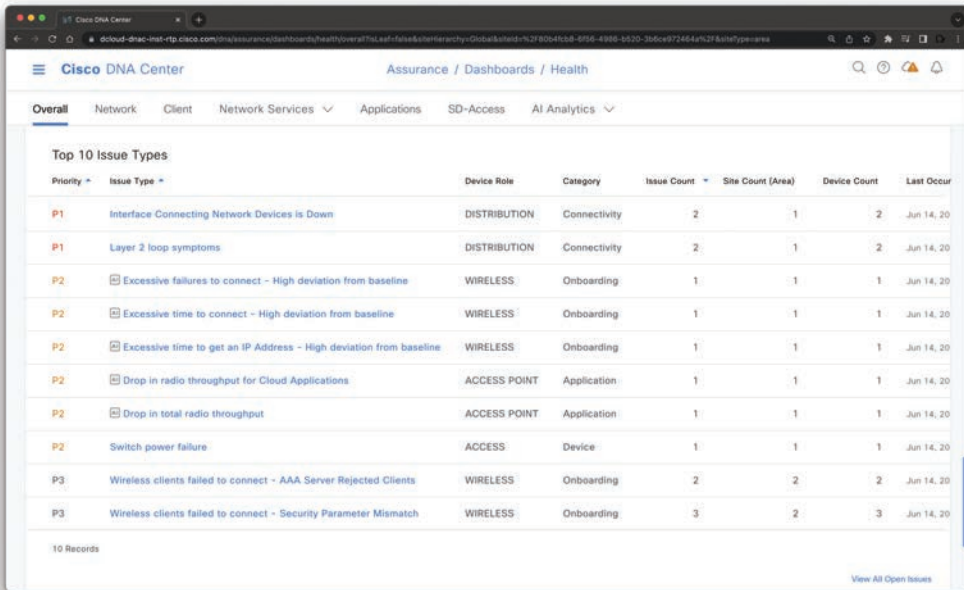


Figure 3-24 The Cisco DNA Center Assurance Top 10 Issues Types

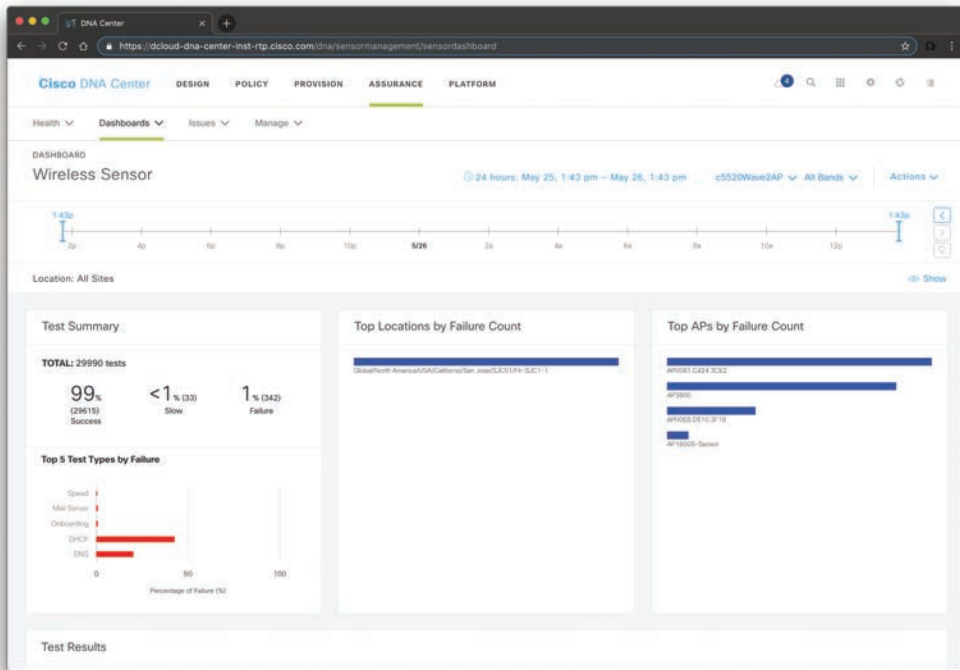


Figure 3-25 The Cisco DNA Center Wireless and Wired Client Statistics

**Key
Topic****Cisco DNA Center APIs**

One of the key benefits of the Cisco DNA Center is the comprehensive available APIs (aka Intent APIs). The Intent APIs are northbound REST APIs that expose specific capabilities of the Cisco DNA Center platform. These APIs provide policy-based abstraction of business intent, allowing you to focus on an outcome to achieve instead of struggling with the mechanisms that implement that outcome. The APIs conform to the REST API architectural style and are simple, extensible, and secure to use.

Cisco DNA Center also has several integration APIs. These integration capabilities are part of westbound interfaces. Cisco DNA Center also allows administrators to manage their non-Cisco devices. Multivendor support comes to Cisco DNA Center through the use of an SDK that can be used to create device packages for third-party devices. A device package enables Cisco DNA Center to communicate with third-party devices by mapping Cisco DNA Center features to their southbound protocols.

TIP Cisco has very comprehensive documentation and tutorials about the Cisco DNA Center APIs at DevNet (<https://developer.cisco.com/dnacenter>).

Cisco DNA Center also has several events and notifications services that allow you to capture and forward Cisco DNA Assurance and Automation (SWIM) events to third-party applications via a webhook URL.

All Cisco DNA Center APIs conform to the REST API architectural styles.

NOTE A REST endpoint accepts and returns HTTPS messages that contain JavaScript Object Notation (JSON) documents. You can use any programming language to generate the messages and the JSON documents that contain the API methods. These APIs are governed by the Cisco DNA Center Role-Based Access Control (RBAC) rules and as a security measure require the user to authenticate successfully prior to using the API.

You can view information about all the Cisco DNA Center APIs by clicking the **Platform** tab and navigating to **Developer Toolkit > APIs**.

**Key
Topic**

TIP All REST requests in Cisco DNA Center require authentication. The Authentication API generates a security token that encapsulates the privileges of an authenticated REST caller. All requested operations are authorized by Cisco DNA Center according to the access privileges associated with the security token that is sent in the request.

Cisco is always expanding the capabilities of the Cisco DNA Center APIs. Please study and refer to the following API documentation and tutorials for the most up-to-date capabilities: <https://developer.cisco.com/docs/dna-center> and <https://developer.cisco.com/site/dna-center-rest-api>.

Cisco DNA Security Solution**Key
Topic**

The Cisco DNA Security solution supports several other security products and operations that allow you to detect and contain cybersecurity threats. One of the components of the

Cisco DNA Security solution is the Encrypted Traffic Analytics (ETA) solution. Cisco ETA allows you to detect security threats in encrypted traffic without decrypting the packets. It is able to do this by using machine learning and other capabilities. To use Encrypted Traffic Analytics, you need one of the following network devices along with Cisco Secure Network Analytics (formerly known as Stealthwatch):

- Catalyst 9000 switches
- ASR 1000 Series routers
- ISR 4000 Series routers
- CSR 1000V Series virtual routers
- ISR 1000 Series routers
- Catalyst 9800 Series wireless controllers

Cisco Secure Network Analytics provides network visibility and security analytics to rapidly detect and contain threats. You will learn more about the Cisco Secure Network Analytics solution in Chapter 5, “Network Visibility and Segmentation.”

As you learned in previous sections of this chapter, the Cisco TrustSec solution and Cisco ISE enable you to control networkwide access, enforce security policies, and help meet compliance requirements.

Cisco DNA Multivendor Support

Cisco DNA Center now allows customers to manage their non-Cisco devices. Multivendor support comes to Cisco DNA Center through the use of an SDK that can be used to create device packages for third-party devices. A device package enables Cisco DNA Center to communicate with third-party devices by mapping Cisco DNA Center features to their southbound protocols. Multivendor support capabilities are based on southbound interfaces. These interfaces interact directly with network devices by means of CLI, SNMP, or NETCONF.

NOTE Southbound interfaces are not exposed to the consumer. Instead, the consumer uses Intent APIs, which abstract the underlying complexity of the traditional network. The user of Intent APIs need not be concerned with the particular protocols that the southbound interfaces use to implement network intent on devices that Cisco DNA Center supports.

Introduction to Network Programmability

As you were able to see in previous sections of this chapter, learning to code and work with programmable infrastructures is very important in today’s environment. You saw the value of using APIs. Whether you have configured large networks in the past or are just getting started, you know that this probably involved a lot of clicking, typing, copying-and-pasting, and many repetitive tasks. Nowadays, modern APIs enable you to complete powerful tasks, reduce all the repetitive work, and save time.

Using APIs, you can make requests like the ones shown in Figure 3-26 in a very simple way.

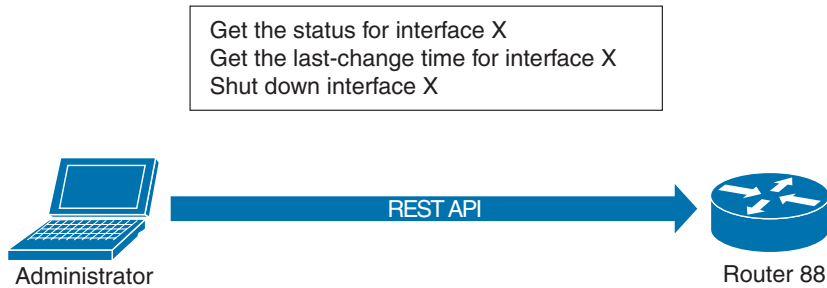


Figure 3-26 Using Network Infrastructure Device APIs

Key Topic

Modern Programming Languages and Tools

Modern programming languages like JavaScript, Python, Go, Swift, and others are more flexible and easier to learn than their predecessors. You might wonder what programming language you should learn first. Python is one of the programming languages recommended to learn first—not only for network programmability, but for many other scenarios.

TIP Many different sites allow you to get started with Python. The following are several great resources to learn Python:

- Learn Python dot org: <https://www.learnpython.org>
- W3 Schools Python tutorials: <https://www.w3schools.com/python/>
- The Python Tutorial: <https://docs.python.org/3/tutorial/>

Combining programming capabilities with developer tools like Git (GitHub or GitLab repositories), package management systems, virtual environments, and integrated development environments (IDEs) allows you to create your own set of powerful tools and workflows.

Another amazing thing is the power of code reuse and online communities. In the past, when you wanted to create some program, you often had to start “from scratch.” For example, if you wanted to just make an HTTPS web request, you had to create code to open a TCP connection over port 443, perform the TLS negotiation, exchange and validate certificates, and format and interpret HTTP requests and responses.

Nowadays, you can just use open-source software in GitHub or simply use packages such as the Python requests package, as shown in Figure 3-27.

In Figure 3-27, the Python package called *requests* is installed using the package manager for Python called *pip* (<https://pypi.org/project/pip>). The requests library allows you to make HTTP/HTTPS requests in Python very easily.

Now that you have the requests package installed, you can start making HTTP requests, as shown in Figure 3-28.

```

[omar@omar_server_1] ~
└─# pip install requests
Collecting requests
  Downloading https://files.pythonhosted.org/packages/51/bd/23c926cd341ea6b7dd0b2a00aba99ae0f828be89d72b2190f27c11d4b7fb/requests-2.22.0-py2.py3-none-any.whl (57kB)
    |-----| 61kB 2.2MB/s
Requirement already satisfied: urllib3!=1.25.0,!=1.25.1,<1.26,>=1.21.1 in /usr/local/lib/python3.7/site-packages (from requests) (1.24.1)
Collecting chardet<3.1.0,>=3.0.2 (from requests)
  Downloading https://files.pythonhosted.org/packages/bc/a9/01ffebfb562e4274b6487b4bb1ddec7ca55ec7510b22e4c51f14098443b8/chardet-3.0.4-py2.py3-none-any.whl (133kB)
    |-----| 143kB 7.9MB/s
Collecting idna<2.9,>=2.5 (from requests)
  Downloading https://files.pythonhosted.org/packages/14/2c/cd551d81dbe15200be1cf41cd03869a46fe7226e7450af7a6545bfc474c9/idna-2.8-py2.py3-none-any.whl (58kB)
    |-----| 61kB 9.2MB/s
Requirement already satisfied: certifi>=2017.4.17 in /usr/local/lib/python3.7/site-packages (from requests) (2018.11.29)
Installing collected packages: chardet, idna, requests
Successfully installed chardet-3.0.4 idna-2.8 requests-2.22.0
[omar@omar_server_1] ~
└─#

```

Figure 3-27 *Installing the Python Requests Package Using pip*

```

[omar@omar_server_1] ~
└─$ python
Python 3.7.0 (default, Sep 5 2018, 03:25:31)
[GCC 6.3.0 20170516] on linux
Type "help", "copyright", "credits" or "license()" for more information.
>>> import requests
>>> requests.get("https://h4cker.org")
<Response [200]>
>>>

```

Figure 3-28 *Using the Python Requests Package*

In Figure 3-28, the interactive Python shell (interpreter) is used to use (import) the requests package and send an HTTP GET request to the website at <https://h4cker.org>. The HTTP GET request is successful and the 200 message/response is shown.

Additional information about the Python interpreter can be found at <https://docs.python.org/3/tutorial/interpreter.html> and https://www.python-course.eu/python3_interactive.php.

TIP The W3 schools website has a very good explanation of the HTTP status code messages at https://www.w3schools.com/tags/ref_httpmessages.asp.

The HTTP status code messages can be in the following ranges:

- Messages in the 100 range are informational.
- Messages in the 200 range are related to successful transactions.
- Messages in the 300 range are related to HTTP redirections.
- Messages in the 400 range are related to client errors.
- Messages in the 500 range are related to server errors.

When HTTP servers and browsers communicate with each other, they perform interactions based on headers as well as body content. The HTTP Request has the following structure:

1. The METHOD, which in this example is an HTTP GET. However, the HTTP methods can be the following:
 - **GET:** Retrieves information from the server.
 - **HEAD:** Basically, this is the same as a GET, but it returns only HTTP headers and no document body.
 - **POST:** Sends data to the server (typically using HTML forms, API requests, and the like).
 - **TRACE:** Does a message loopback test along the path to the target resource.
 - **PUT:** Uploads a representation of the specified URI.
 - **DELETE:** Deletes the specified resource.
 - **OPTIONS:** Returns the HTTP methods that the server supports.
 - **CONNECT:** Converts the request connection to a transparent TCP/IP tunnel.
2. The URI and the path-to-resource field represent the path portion of the requested URL.
3. The request version-number field specifies the version of HTTP used by the client.
4. The user agent is Chrome in this example, and it was used to access the website. In the packet capture, you see the following:


```
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_4)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.181
Safari/537.36\r\n.
```
5. Next, you see several other fields like accept, accept-language, accept encoding, and others.
6. The server, after receiving this request, generates a response.

- The server response has a three-digit status code and a brief human-readable explanation of the status code. Then below you see the text data (which is the HTML code coming back from the server and displaying the website contents).

TIP The requests Python package is used often to interact with APIs. You can obtain more information about the requests Python package at <https://realpython.com/python-requests> and <https://developer.cisco.com/learning/labs/dne-intro-python-basics/introduction/>.

Key Topic

DevNet

DevNet is a platform created by Cisco that has numerous resources for network and application developers. DevNet is an amazing resource that includes many tutorials, free video courses, sandboxes, learning paths, and sample code to interact with many APIs. You can access DevNet at developer.cisco.com.

If you are new to programming and network programmability, you can take advantage of the following DevNet tutorials and learning paths:

- Introduction to Coding and APIs: <https://developer.cisco.com/startnow>
- Network Programmability Basics Video Course: <https://developer.cisco.com/video/net-prog-basics/>
- Parsing JSON using Python: <https://developer.cisco.com/learning/lab/coding-202-parsing-json/step/1>
- DevNet GitHub Repositories: <https://github.com/CiscoDevNet>
- DevNet Developer Videos: <https://developer.cisco.com/video>
- DevNet Git Tutorials: <https://developer.cisco.com/learning/lab/git-intro/step/1>
- DevNet ACI Programmability: <https://developer.cisco.com/learning/tracks/aci-programmability>
- Build Applications with Cisco: <https://developer.cisco.com/learning/tracks/app-dev>
- IOS-XE Programmability: <https://developer.cisco.com/learning/tracks/iosxe-programmability>
- Network Programmability for Network Engineers: <https://developer.cisco.com/learning/tracks/netprog-eng>

Key Topic

Getting Started with APIs

APIs are used everywhere these days. A large number of modern applications use some type of APIs because they make access available to other systems to interact with the application. There are few methods or technologies behind modern APIs:

- **Simple Object Access Protocol (SOAP):** SOAP is a standards-based web services access protocol that was originally developed by Microsoft and has been used by numerous legacy applications for many years. SOAP exclusively uses XML to provide API services. XML-based specifications are governed by XML Schema Definition (XSD) documents. SOAP was originally created to replace older solutions such as

the Distributed Component Object Model (DCOM) and Common Object Request Broker Architecture (CORBA). You can find the latest SOAP specifications at <https://www.w3.org/TR/soap>.

- **Representational State Transfer (REST):** REST is an API standard that is easier to use than SOAP. It uses JSON instead of XML, and it uses standards like Swagger and the OpenAPI Specification (<https://www.openapis.org>) for ease of documentation and to help with adoption.
- **GraphQL and queryable APIs:** This is another query language for APIs that provides many developer tools. GraphQL is now used for many mobile applications and online dashboards. Many languages support GraphQL. You can learn more about GraphQL at <https://graphql.org/code>.

NOTE SOAP and REST share similarities over the HTTP protocol. SOAP limits itself to a stricter set of API messaging patterns than REST.

APIs often provide a roadmap describing the underlying implementation of an application. API documentation can provide a great level of detail that can be very valuable to security professionals. These types of documentation include the following:

- **Swagger (OpenAPI):** Swagger is a modern framework of API documentation and is now the basis of the OpenAPI Specification (OAS). Additional information about Swagger can be obtained at <https://swagger.io>. The OAS specification is available at <https://github.com/OAI/OpenAPI-Specification>.
- **Web Services Description Language (WSDL) documents:** WSDL is an XML-based language that is used to document the functionality of a web service. The WSDL specification can be accessed at <https://www.w3.org/TR/wsdl20-primer>.
- **Web Application Description Language (WADL) documents:** WADL is also an XML-based language for describing web applications. The WADL specification can be obtained from <https://www.w3.org/Submission/wadl>.

NOTE Most Cisco products and services use RESTful (REST) APIs.

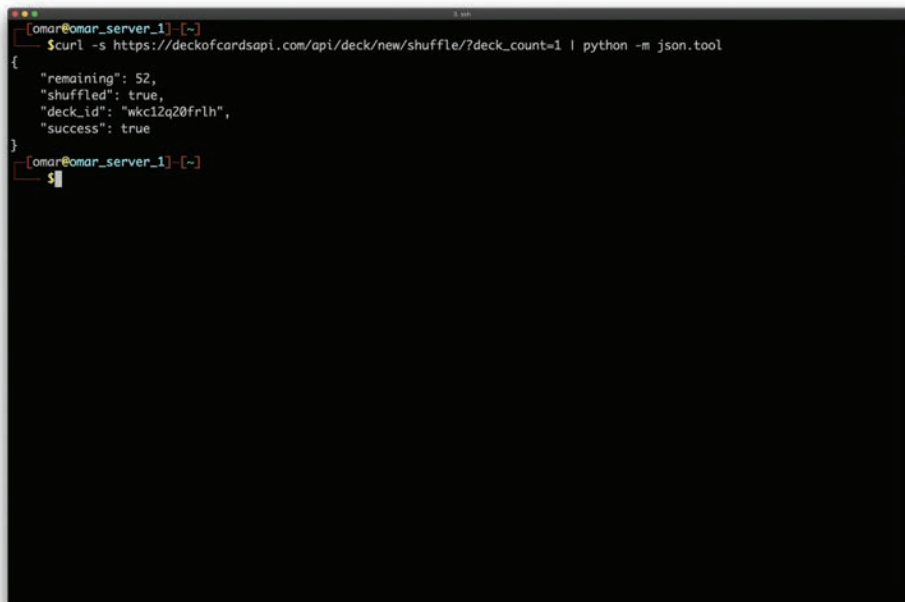


REST APIs

Let's take a look at a quick example of a REST API. There is a sample API you can use to perform several tests at <https://deckofcardsapi.com>. In Figure 3-29, the Linux `curl` utility is used to retrieve a “new deck of cards” from the Deck of Cards API. The API “shuffles” a deck of cards for you. The deck ID (`deck_id`) is `wkc12q20frlh` in this example.

NOTE The `python -m json.tool` command is used to invoke the `json.tool` Python module to “pretty print” the JSON output. You can obtain more information about the `json.tool` Python module at <https://docs.python.org/3/library/json.html#module-json.tool>.

Suppose that you want to draw a random card from the deck. Since you have the deck ID, you can easily use the command shown in Figure 3-30 to draw a random card.



```
[omar@omar_server_1] ~$ curl -s https://deckofcardsapi.com/api/deck/new/shuffle/?deck_count=1 | python -m json.tool
{
  "remaining": 52,
  "shuffled": true,
  "deck_id": "wkc12q20frlh",
  "success": true
}
[omar@omar_server_1] ~$
```

Figure 3-29 Using curl to Obtain Information from an API



```
[omar@omar_server_1] ~$ curl -s https://deckofcardsapi.com/api/deck/new/shuffle/?deck_count=1 | python -m json.tool
{
  "remaining": 52,
  "shuffled": true,
  "deck_id": "wkc12q20frlh",
  "success": true
}
[omar@omar_server_1] ~$ curl -s https://deckofcardsapi.com/api/deck/wkc12q20frlh/draw/ | python -m json.tool
{
  "remaining": 51,
  "cards": [
    {
      "code": "9S",
      "suit": "SPADES",
      "value": "9",
      "images": {
        "png": "https://deckofcardsapi.com/static/img/9S.png",
        "svg": "https://deckofcardsapi.com/static/img/9S.svg"
      },
      "image": "https://deckofcardsapi.com/static/img/9S.png"
    }
  ],
  "deck_id": "wkc12q20frlh",
  "success": true
}
[omar@omar_server_1] ~$
```

Figure 3-30 Using curl to Obtain Additional Information from the Deck of Cards API

You can see the response (in JSON), including the remaining number of cards and the card that was retrieved (the 9 of spades). Other information, such as the code, suit, value, and images of the card, is also included in the JSON output.

Example 3-1 shows a Python script that you can use to interact with the Deck of Cards API.

Example 3-1 *Sample Python Script to Interact with the Deck of Cards API*

```
#!/usr/bin/python
import requests

deck_id = None

def create_deck():
    global deck_id
    deck_url = "https://deckofcardsapi.com/api/deck/new/"
    deck_response = requests.get(deck_url)
    deck_data = deck_response.json()
    deck_id = deck_data['deck_id']
    print("New deck created with ID:", deck_id)

def shuffle_deck():
    shuffle_url = f"https://deckofcardsapi.com/api/deck/{deck_id}/shuffle/"
    requests.get(shuffle_url)
    print("Deck shuffled")

def draw_card():
    draw_url = f"https://deckofcardsapi.com/api/deck/{deck_id}/draw?count=1"
    draw_response = requests.get(draw_url)
    draw_data = draw_response.json()
    if len(draw_data['cards']) > 0:
        card = draw_data['cards'][0]
        print("The card is a {} of {}".format(card['value'], card['suit']))
    else:
        print("No more cards in the deck")

def add_jokers():
    jokers_url = f"https://deckofcardsapi.com/api/deck/{deck_id}/jokers?count=2"
    requests.get(jokers_url)
    print("Jokers added to the deck")

# Display the menu
while True:
    print("Omar's Example with the Deck of Cards API. Please select from the following menu:")
    print("1. Create a new deck")
    print("2. Shuffle the deck")
```

```
print("3. Draw a card")
print("4. Add jokers to the deck")
print("5. Quit")

choice = input("Enter your choice: ")

if choice == "1":
    create_deck()
elif choice == "2":
    shuffle_deck()
elif choice == "3":
    draw_card()
elif choice == "4":
    add_jokers()
elif choice == "5":
    print("Goodbye!")
    break
else:
    print("Invalid choice. Please try again.")
```

The script in Example 3-1 starts by importing the requests module, which is used to send HTTP requests to the Deck of Cards API. If you do not have the requests module installed, you can easily install it with the `pip3 install requests` command. The script defines a global variable called `deck_id`, which will store the ID of the deck that the user creates. It also defines four functions: `create_deck()`, `shuffle_deck()`, `draw_card()`, and `add_jokers()`. Each function corresponds to one of the actions that the user can select from the menu.

The `create_deck()` function sends an HTTP GET request to the API endpoint `https://deckofcardsapi.com/api/deck/new/` to create a new deck of cards. It then extracts the ID of the deck from the JSON response and saves it in the `deck_id` variable. The `shuffle_deck()` function sends an HTTP GET request to the API endpoint `https://deckofcardsapi.com/api/deck/{deck_id}/shuffle/` to shuffle the deck. The `draw_card()` function sends an HTTP GET request to the API endpoint `https://deckofcardsapi.com/api/deck/{deck_id}/draw/?count=1` to draw a single card from the deck. It extracts information about the card from the JSON response and prints it to the console. The `add_jokers()` function sends an HTTP GET request to the API endpoint `https://deckofcardsapi.com/api/deck/{deck_id}/jokers/?count=2` to add two jokers to the deck.

The script defines a menu that displays the available actions to the user and prompts the user to enter a choice. It uses a while loop to repeatedly display the menu to the user until the user chooses to quit. When the user selects an action from the menu, the script executes the appropriate function based on the user's choice. After sending the HTTP request, each function extracts information from the JSON response, if necessary, and prints a message to the console indicating that the action was completed. If the user enters an invalid choice, the script prints an error message to the console and displays the menu again.

NOTE The DevNet tutorial at the following link shows how to interact with this sample API using Postman: <https://developer.cisco.com/learning/labs/dne-postman-code/using-postman-to-generate-python-code/>.

Using Network Device APIs

Earlier in this chapter you learned that there are several API resources available in many Cisco solutions such as the Cisco DNA Center. The following are a few basic available API resources on the Cisco DNA Center Platform (10.1.1.1 is the IP address of the Cisco DNA Center):

- **https://10.1.1.1/api/system/v1/auth/token:** Used to get and encapsulate user identity and role information as a single value.
- **https://10.1.1.1/api/v1/network-device:** Used to get the list of the first 500 network devices sorted lexicographically based on host name.
- **https://10.1.1.1/api/v1/interface:** Used to get information about every interface on every network device.
- **https://10.1.1.1/api/v1/host:** Used to get the name of a host, the ID of the VLAN that the host uses, the IP address of the host, the MAC address of the host, the IP address of the network device to which the host is connected, and more.
- **https://10.1.1.1/api/v1/flow-analysis:** Used to trace a path between two IP addresses. The function will wait for analysis to complete, and return the results.

There are a dozen (or dozens?) more APIs that you can use and interact with Cisco DNA Center at <https://developer.cisco.com/dnacentr>. Many other Cisco products include APIs that can be used to integrate third-party applications, obtain information similar to the preceding examples, as well as change the configuration of the device, apply policies, and more. Many of those APIs are also documented in DevNet (developer.cisco.com).

Modern networking devices support programmable capabilities such as NETCONF, RESTCONF, and YANG models. The following sections provide details about these technologies.



YANG Models

YANG is an API contract language used in many networking devices. In other words, you can use YANG to write a specification for what the interface between a client and networking device (server) should be on a particular topic. YANG was originally defined in RFC 6020 (<https://tools.ietf.org/html/rfc6020>).

TIP A specification written in YANG is referred to as a “YANG module.” A collection (or set) of YANG modules is often called a “YANG model.”

A YANG model typically concentrates on the data that a client processes using standardized operations.

NOTE Keep in mind that in NETCONF and RESTCONF implementations, the YANG controller is the client and the network elements are the server. You will learn more about NETCONF and RESTCONF later in this chapter.

Figure 3-31 shows an example of a network management application (client) interacting with a router (server) using YANG as the API contract.



Figure 3-31 A Basic YANG Example

A YANG-based server (as shown in Figure 3-31) publishes a set of YANG modules, which taken together form the system's YANG model. The YANG modules specify what a client can do. The following are a few examples of what a client can do using different YANG models:

- **Configure:** For example, enabling a routing protocol or a particular interface.
- **Receive notifications:** An example of notifications can be repeated login failures, interface failures, and so on.
- **Monitor status:** For example, retrieving information about CPU and memory utilization, packet counters, and so on.
- **Invoke actions:** For instance, resetting packet counters, rebooting the system, and so on.

NOTE The YANG model of a device is often called a “schema” defining the structure and content of messages exchanged between the application and the device.

The YANG language provides flexibility and extensibility capabilities that are not present in other model languages. When you create new YANG modules, you can leverage the data hierarchies defined in other modules. YANG also permits new statements to be defined, allowing the language itself to be expanded in a consistent way.

TIP DevNet has a series of videos that demonstrates how YANG works at https://developer.cisco.com/video/net-prog-basics/02-network_device_apis/yang.



NETCONF

NETCONF is defined in RFCs 6241 and 6242. NETCONF was created to overcome the challenges in legacy Simple Network Management Protocol (SNMP) implementations.

A NETCONF client typically has the role of a network management application. The NETCONF server is a managed network device (router, switch, and so on). You can also have intermediate systems (often called “controllers”) that control a particular aspect or domain. Controllers can act as a server to its managers and as a client to its networking devices, as shown in Figure 3-32.

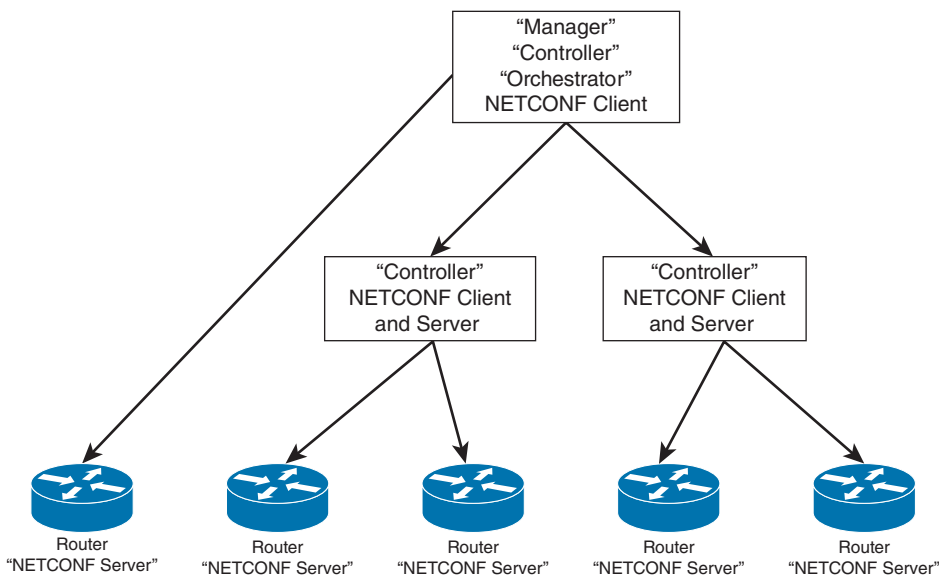


Figure 3-32 NETCONF Clients, Servers, and Controllers

In Figure 3-32, a node called a “Manager” manages a NETCONF server (router) and two “Controllers,” which are both a server for the Manager and a client for the other network devices (routers).

NOTE NETCONF was created before YANG. Other languages were used for NETCONF operations. On the other hand, YANG is the only language widely used for NETCONF nowadays.

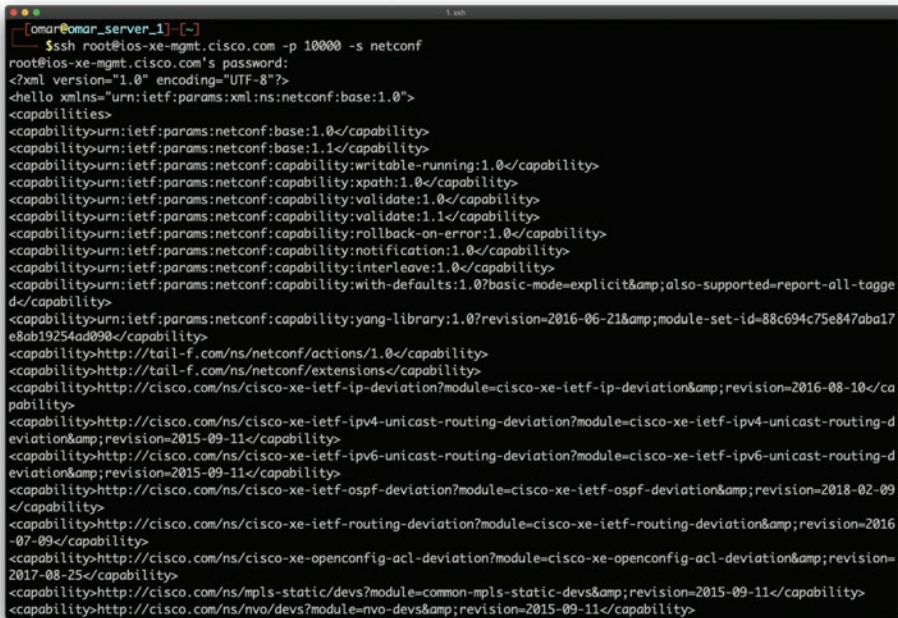
NETCONF sessions established from a NETCONF client to a NETCONF server consist of a sequence of messages. Both parties send a “hello” message when they initially connect. All message exchanges are initiated by the NETCONF client. The hello message includes which NETCONF protocol version(s) the devices support. The server states which optional capabilities it supports.

NETCONF messages are either a remote procedure call (RPC) or an “rpc-reply.” Each RPC is a request from the client to the server to execute a given operation. The NETCONF rpc-reply is sent by the server when it has completed or failed to complete the request. Some NETCONF rpc-replies are short answers to a simple query, or just an OK that the order was

executed. Some are long and may contain the entire device configuration or status. NETCONF rpc-replies to subscriptions consist of a message that technically never ends. Other information of the rpc-reply is generated by the server. A NETCONF rpc-reply may also be a NETCONF rpc-error, indicating that the requested operation failed.

NETCONF messages are encoded in an XML-based structure defined by the NETCONF standard. The NETCONF communication is done over Secure Shell (SSH), but using a default TCP port 830. This can be configured to a different port.

SSH supports a subsystem concept. NETCONF has its own subsystem: netconf. Figure 3-33 shows how you can connect to a networking device (in this case, a CSR-1000v router configured with the hostname `ios-xe-mgmt.cisco.com`). The username of the router is `root`. You are also asked to provide a password. The router is configured for NETCONF over TCP port 10000.



```

omar@omar_server_1 [~]
└─$ ssh root@ios-xe-mgmt.cisco.com -p 10000 -s netconf
root@ios-xe-mgmt.cisco.com's password:
<?xml version="1.0" encoding="UTF-8"?>
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<capabilities>
<capability>urn:ietf:params:netconf:base:1.0</capability>
<capability>urn:ietf:params:netconf:base:1.1</capability>
<capability>urn:ietf:params:netconf:capability:writable-running:1.0</capability>
<capability>urn:ietf:params:netconf:capability:xpath:1.0</capability>
<capability>urn:ietf:params:netconf:capability:validate:1.0</capability>
<capability>urn:ietf:params:netconf:capability:validate:1.1</capability>
<capability>urn:ietf:params:netconf:capability:rollback-on-error:1.0</capability>
<capability>urn:ietf:params:netconf:capability:notification:1.0</capability>
<capability>urn:ietf:params:netconf:capability:interleave:1.0</capability>
<capability>urn:ietf:params:netconf:capability:with-defaults:1.0?basic-mode=explicit&also-supported=report-all-tagged</capability>
<capability>urn:ietf:params:netconf:capability:yang-library:1.0?revision=2016-06-21&module-set-id=88c694c75e847aba17e8ab19254ad0990</capability>
<capability>http://tail-f.com/ns/netconf/actions/1.0</capability>
<capability>http://tail-f.com/ns/netconf/extensions</capability>
<capability>http://cisco.com/ns/cisco-xe-ietf-ip-deviation?module=cisco-xe-ietf-ip-deviation&revision=2016-08-10</capability>
<capability>http://cisco.com/ns/cisco-xe-ietf-ipv4-unicast-routing-deviation?module=cisco-xe-ietf-ipv4-unicast-routing-deviation&revision=2015-09-11</capability>
<capability>http://cisco.com/ns/cisco-xe-ietf-ipv6-unicast-routing-deviation?module=cisco-xe-ietf-ipv6-unicast-routing-deviation&revision=2015-09-11</capability>
<capability>http://cisco.com/ns/cisco-xe-ietf-ospf-deviation?module=cisco-xe-ietf-ospf-deviation&revision=2018-02-09</capability>
<capability>http://cisco.com/ns/cisco-xe-ietf-routing-deviation?module=cisco-xe-ietf-routing-deviation&revision=2016-07-09</capability>
<capability>http://cisco.com/ns/cisco-xe-openconfig-acl-deviation?module=cisco-xe-openconfig-acl-deviation&revision=2017-08-25</capability>
<capability>http://cisco.com/ns/mpls-static/devs?module=common-mpls-static-devs&revision=2015-09-11</capability>
<capability>http://cisco.com/ns/nvo/devs?module=nvo-devs&revision=2015-09-11</capability>

```

Figure 3-33 Using the NETCONF SSH Subsystem

TIP DevNet has several sandboxes where you can practice these concepts and more at <https://devnetsandbox.cisco.com>.

An open-source Python library for NETCONF clients called `ncclient` is available on GitHub at <https://github.com/ncclient/ncclient>. You can install it using Python `pip`, as shown here:

```
pip install ncclient
```

There are several sample scripts at the DevNet GitHub repositories that can help you get started at https://github.com/CiscoDevNet/python_code_samples_network.

RESTCONF



You already learned that REST is a type of modern API. Many network administrators wanted to have the capabilities of NETCONF over “REST.” This is why a REST-based variant of NETCONF was created. RESTCONF is now supported in many networking devices in the industry.

RESTCONF is defined in RFC 8040 and it follows the REST principles. However, not all REST-based APIs are compatible or even comparable to RESTCONF.

The RESTCONF interface is built around a small number of standardized requests (GET, PUT, POST, PATCH, and DELETE). Several of the REST principles are similar to NETCONF:

- The client-server model
- The layered system principle
- The first two uniform interface principles

One of the differences between RESTCONF and NETCONF is the stateless server principle. NETCONF is based on clients establishing a session to the server (which is not stateless). NETCONF clients frequently connect and then manipulate the candidate datastore with a number of *edit-config* operations. The NETCONF clients may also send a *validation* call to NETCONF servers. This is different in RESTCONF.

RESTCONF requires the server to keep some client state. Any request the RESTCONF client sends is acted upon by the server immediately. You cannot send any transactions that span multiple RESTCONF messages. Subsequently, some of the key features of NETCONF (including networkwide transactions) are not possible in RESTCONF.

Let’s take a look at a quick example of using RESTCONF. Example 3-2 shows a Python script that is used to obtain the details of all interfaces in a networking device using RESTCONF.

Example 3-2 Python Script to Retrieve Interface Details from a Networking Device Using RESTCONF

```
#!/usr/bin/python
import requests
import sys

# disable warnings from SSL/TLS certificates
requests.packages.urllib3.disable_warnings()

# the IP address or hostname of the networking device
HOST = 'ios-xe-mgmt.cisco.com'

# use your user credentials to access the networking device
USER = 'root'
PASS = 'supersecretpassword'
```

```

# create a main() method
def main():
    """Main method that retrieves the interface details from a
    networking device via RESTCONF."""

    # RESTCONF url of the networking device
    url="https://{h}:9443/restconf/data/ietf-
    interfaces:interfaces".format(h=HOST)

    # RESTCONF media types for REST API headers
    headers = {'Content-Type': 'application/yang-data+json',
              'Accept': 'application/yang-data+json'}

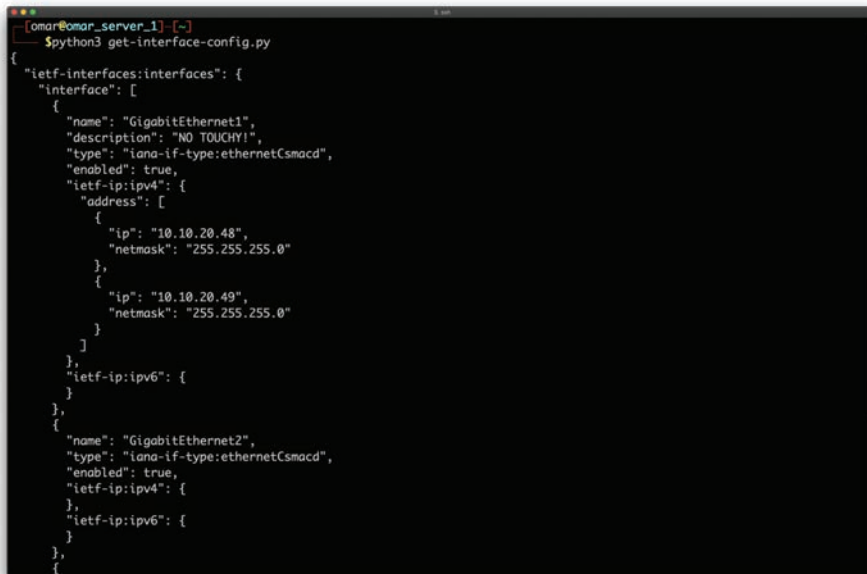
    # this statement performs a GET on the specified url
    response = requests.get(url, auth=(USER, PASS),
                            headers=headers, verify=False)

    # print the json that is returned
    print(response.text)

if __name__ == '__main__':
    sys.exit(main())

```

Figure 3-34 shows the output of the Python script, including the information of all the interfaces in that networking device (`ios-xe-mgmt.cisco.com`).



```

[omar@omar_server_1] [-]
$python3 get-interface-config.py
{"ietf-interfaces:interfaces": {
  "interface": [
    {
      "name": "GigabitEthernet1",
      "description": "NO TOUCHY!",
      "type": "iana-if-type:ethernetCsmacd",
      "enabled": true,
      "ietf-ip:ipv4": {
        "address": [
          {
            "ip": "10.10.20.48",
            "netmask": "255.255.255.0"
          },
          {
            "ip": "10.10.20.49",
            "netmask": "255.255.255.0"
          }
        ]
      },
      "ietf-ip:ipv6": {
      }
    },
    {
      "name": "GigabitEthernet2",
      "type": "iana-if-type:ethernetCsmacd",
      "enabled": true,
      "ietf-ip:ipv4": {
      },
      "ietf-ip:ipv6": {
      }
    }
  ]
}

```

Figure 3-34 Using Python to Obtain Information from a Network Device Using RESTCONF

TIP Watch the DevNet “Getting Started with Network Device APIs” video for additional step-by-step information about Network APIs, NETCONF, RESTCONF, and YANG at https://developer.cisco.com/video/net-prog-basics/02-network_device_apis.

OpenConfig and gNMI

The OpenConfig consortium (<https://github.com/openconfig>) is a collaborative effort to provide vendor-neutral data models (in YANG) for network devices. OpenConfig uses the gRPC Network Management Interface (gNMI). The following GitHub repository includes detailed information about gNMI, as well as sample code (<https://github.com/openconfig/gnmi>).

NOTE The gRPC specification (<https://grpc.io>) is a modern Remote Procedure Call (RPC) framework. RPC allows a client to invoke operations (also called “procedures”) on a server. RPC includes an interface description language (IDL) used to state what procedures the server supports (including the input and output data from them). RPC also uses client libraries to call upon those procedures (supported in different programming languages). RPC uses a serialization, marshalling, and transport mechanism for the messages (generally called an RPC protocol).

The gNMI protocol is similar to NETCONF and RESTCONF. gNMI uses YANG models, but it can be used with other interface description languages (IDLs). The OpenConfig consortium defined several standard YANG models to go with the protocols. These YANG models describe many essential networking features such as interface configuration, routing protocols, QoS, Wi-Fi configurations, and more.

Exam Preparation Tasks

As mentioned in the section “Book Features” in the Introduction, you have a couple of choices for exam preparation: the exercises here, Chapter 12, “Final Preparation,” and the exam simulation questions in the Pearson Test Prep Software Online.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topic icon in the outer margin of the page. Table 3-2 lists these key topics and the page numbers on which each is found.



Table 3-2 Key Topics for Chapter 3

| Key Topic Element | Description | Page Number |
|-------------------|--|-------------|
| Section | Traditional Networking Planes | 113 |
| Section | So What’s Different with SDN? | 114 |
| Section | Introduction to the Cisco ACI Solution | 114 |
| List | Understand the functions of the APIC | 116 |
| Section | VXLAN and Network Overlays | 116 |
| Paragraph | Understand what is micro-segmentation | 118 |

| Key Topic Element | Description | Page Number |
|-------------------|--|-------------|
| Paragraph | Understand “east-west” traffic and “north-south” traffic | 118 |
| Section | Open-Source Initiatives | 120 |
| Paragraph | Understand northbound and southbound APIs | 121 |
| Section | More About Network Function Virtualization | 121 |
| Section | Cisco DNA Center APIs | 135 |
| Tip | Cisco DNA Center APIs in DevNet | 135 |
| Section | Cisco DNA Security Solution | 135 |
| Section | Modern Programming Languages and Tools | 137 |
| Section | DevNet | 140 |
| Section | Getting Started with APIs | 140 |
| Section | REST APIs | 141 |
| Section | YANG Models | 145 |
| Section | NETCONF | 147 |
| Section | RESTCONF | 149 |

Define Key Terms

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

Representational State Transfer (REST), Simple Object Access Protocol (SOAP), Contiv, Network Functions Virtualization (NFV), Neutron, Open vSwitch, OpenDaylight (ODL), YANG, NETCONF, RESTCONF

Review Questions

- The RESTCONF interface is built around a small number of standardized requests. Which of the following are requests supported by RESTCONF?
 - GET
 - PUT
 - PATCH
 - All of these answers are correct.
- NETCONF messages are encoded in a(n) _____ structure defined by the NETCONF standard.
 - JSON
 - XML
 - OWASP
 - RESTCONF

3. Which of the following is a Cisco resource where you can learn about network programmability and obtain sample code?
 - a. APIC
 - b. ACI
 - c. DevNet
 - d. NETCONF
4. A YANG-based server publishes a set of YANG modules, which taken together form the system's _____.
 - a. YANG model
 - b. NETCONF model
 - c. RESTCONF model
 - d. gRPC model
5. Which of the following HTTP methods sends data to the server typically used in HTML forms and API requests?
 - a. POST
 - b. GET
 - c. TRACE
 - d. PUT
6. Which of the following is a solution that allows you to detect security threats in encrypted traffic without decrypting the packets?
 - a. ETA
 - b. Cisco Secure Email (formerly known as ESA)
 - c. Cisco Secure Web Appliance (formerly known as WSA)
 - d. None of these answers are correct.
7. Which of the following is an open-source project that allows you to deploy micro-segmentation policy-based services in container environments?
 - a. OVS
 - b. Contiv
 - c. ODL
 - d. All of these answers are correct.
8. NFV nodes such as virtual routers and firewalls need which of the following components as an underlying infrastructure?
 - a. A hypervisor
 - b. A virtual forwarder to connect individual instances
 - c. A network controller
 - d. All of these answers are correct.
9. There have been multiple IP tunneling mechanisms introduced throughout the years. Which of the following are examples of IP tunneling mechanisms?
 - a. VXLAN
 - b. SST
 - c. NVGRE
 - d. All of these answers are correct.

- 10.** Which of the following is true about SDN?
- a.** SDN provides numerous benefits in the management plane. These benefits are in both physical switches and virtual switches.
 - b.** SDN changed a few things in the management, control, and data planes. However, the big change was in the control and data planes in software-based switches and routers (including virtual switches inside of hypervisors).
 - c.** SDN is now widely adopted in data centers.
 - d.** All of these answers are correct.

This page intentionally left blank



Index

Symbols

3DES (Triple Digital Encryption Standard), 84, 86, 93, 496
5–9s, 46
6LoWPAN (Low Power Wireless Personal Area Networks), 56
100-500 status code messages, 139
802.1X, 198, 334
 802.1AB, 338–339
 802.1D, 328–332
 802.1Q, 323–326
 802.1w, 332
 configuration, 213–222
 monitor mode, 306
 RADIUS, 213
 roles in, 188–190

A

AAA (authentication, authorization, and accounting), 104, 346
 802.1X. *See* 802.1X
 AAA method lists, 358, 364–369
 access control. *See* access control
 accounting, 104, 179
 authentication. *See* authentication
 authorization. *See* authorization
 Cisco Identity Services Engine. *See* Cisco ISE (Identity Services Engine)
 Cisco pxGrid (Platform Exchange Grid), 193–195

 Cisco TrustSec, 201–203, 306, 310–312
 Diameter, 186–188
 firewalls. *See* firewalls
 infrastructure security. *See* infrastructure security
 overview of, 160–161
 principle of least privilege, 161
 separation of duties, 161
aaa new-model command, 374
aaa type command, 358
ABAC (attribute-based access control), 179
absolute parameter, time-based ACLs (access control lists), 462
acceptable use policy (AUP), 642
access control, 178. *See also* ACLs (access control lists)
 ACE (access control entry), 511, 533–534
 ACM (access control matrix), 181
 attribute-based, 179
 Cisco DNA (Digital Network Architecture). *See* Cisco DNA (Digital Network Architecture)
 Cisco Secure Firewall
 ACLs (*access control lists*) in Cisco ASA, 452–458
 Auto NAT (*Network Address Translation*), 469
 Cisco ASA application inspection, 458–459
 Cisco ASA through-the-box traffic filtering, 456

- Cisco ASA to-the-box traffic filtering*, 459–460
- Cisco Firepower intrusion policies*, 472–478
- ICMP filtering in Cisco ASA*, 462–463
- NAT (Network Address Translation)*, 463–469
- object grouping*, 460–461
- overview of*, 452
- PAT (Port Address Translation)*, 463–469
- policies*, 469–472
- standard ACLs (access control lists)*, 461
- time-based ACLs (access control lists)*, 461–462
- cloud computing, 51
- infrastructure, 179–182
- management, 48–49
- mandatory, 177
- role-based, 135, 178, 354–355, 359
- access point (AP) radios, 133
- ACCESS-ACCEPT, 183–184
- ACCESS-CHALLENGE, 183–184
- access-group command, 460
- access-list command, 461
- ACCESS-REJECT, 183–184
- ACCESS-REQUEST, 183–184
- accounting, 104, 179
- ACCOUNTING-REQUEST, 183
- ACCOUNTING-RESPONSE, 183
- ACE (access control entry), 511, 533–534
- ACI (Application Centric Infrastructure). *See* Cisco ACI (Application Centric Infrastructure)
- ACLs (access control lists)
 - Cisco ASA, 452–458, 533–534
 - Cisco Secure Web Appliance traffic redirection, 647
 - definition of, 179, 335
 - IPv6, 394–395
 - network, 190–191
 - dACLs (downloadable access control lists)*, 191
 - SGACLs (security group ACLs)*, 191
 - standard, 461
 - time-based, 461–462
 - VLAN, 191
 - WebType, 549–550
- ACM (access control matrix), 181
- Active Directory (AD) authentication, 101, 653
- active policy enforcement, 306–310
- Active-Standby failover, Cisco Secure Firewall, 448–450
- Adaptive Security Device Manager (ASDM), 113, 414–415, 423
- Adaptive Security Virtual Appliance (ASAv), 414
- add_jokers() function, 144
- Address Resolution Protocol (ARP), 320, 334, 341–343, 349, 390
- address space layout randomization (ASLR), 42
- addresses
 - IPv6
 - format of*, 383–384
 - types of*, 384–386
 - MAC, 336–338
 - spoofing/proxying, 60
- ADM (Application Dependency Mapping), 622
- admin-context command, 440
- Advanced Encryption Standard (AES), 84, 86, 89, 93, 496
- Advanced Malware Protection (AMP). *See* Cisco Secure Endpoint; Cisco Secure Malware Defense

- Advanced Malware Protection
 - dashboard, Cisco Secure Email, 663
- Advanced Malware Protection Reputation dashboard, Cisco Secure Email, 663–666
- Advanced Message Queuing Protocol (AMQP), 57
- advanced persistent threat (APT), 20
- adversarial examples, 41
- advertising spyware, 27
- AES (Advanced Encryption Standard), 84, 86, 89, 93, 496
- AFL (American Fuzzy Lop), 605
- agents, Cisco Secure Workload, 622
- Aggregation Services Routers (ASRs), 238
- Agile methodology, 583–586
- AH (Authentication Header), 93, 500
- AI (artificial intelligence) vulnerabilities, 40–41
- algorithms. *See* ciphers
- ALGs (application layer gateways), 258
- all-nodes multicast addresses, 384
- all-routers multicast addresses, 384
- Amazon Elastic Kubernetes Service (Amazon EKS), 417
- Amazon Shared Responsibility Model, 605
- Amazon Web Services (AWS), 265, 417
- American Fuzzy Lop (AFL), 605
- AMP (Advanced Malware Protection). *See* Cisco Secure Endpoint; Cisco Secure Malware Defense
- AMP Enabler, 688–689
- AMQP (Advanced Message Queuing Protocol), 57
- analytics
 - Cisco Secure Cloud Analytics, 242, 263–268, 618–619
 - Cisco Secure Network Analytics, 263–264
 - dashboard, 268–270
 - threat hunting with, 270–273
 - malware analysis
 - dynamic, 29–30
 - static, 28
 - anomaly detection, 241–243, 613
- ANSWER, 187
- antidetection routine, 18
- antivirus scanning, 643
- anycast addresses, 385
- Anycast IP, 609
- AnyConnect, 189, 204
- AP (access point) radios, 133
- Apache Mesos, 592
- Apache mod_proxy module, 504
- Apache Struts, 604
- API attacks, 53
- APIC (Application Policy Infrastructure Controller), 114–116
- APIs (application programming interfaces), 140–141
 - Cisco DNA (Digital Network Architecture). *See* Cisco DNA (Digital Network Architecture)
 - documentation, 141
 - gNMI (gRPC Network Management Interface), 151
 - NETCONF, 147–148
 - network device APIs, 145
 - northbound, 121, 135, 136
 - OpenConfig, 151
 - queryable, 141
 - REST APIs, 135, 141–144
 - RESTCONF, 149–151
 - southbound, 121, 136
 - technologies behind, 140–141
 - unprotected, 39–40
 - YANG models, 145
- AppDynamics, 619–622

- application access, 550–551
- application awareness, 120
- Application Centric Infrastructure.
 See Cisco ACI (Application Centric Infrastructure)
- application control, Cisco Secure Endpoint, 683–684
- Application Dependency Mapping (ADM), 622
- application inspection, Cisco ASA, 458–459
- application layer attacks, 389–390
- application layer gateways (ALGs), 258
- application policies, Cisco DNA, 131–132
- Application Policy Infrastructure Controller (APIC), 114–116
- application programming interfaces.
 See APIs (application programming interfaces)
- application sets, 132
- Application Visibility and Control (AVC), 254–255, 257, 642, 655
- application vulnerabilities. *See* vulnerabilities
- application-based segmentation, 299–301
- APT (advanced persistent threat), 20
- Argus, 251
- armoring, ASCII, 42
- ARP (Address Resolution Protocol), 320, 334, 341–343, 349, 390
- artificial intelligence (AI) vulnerabilities, 40–41
- ASA firewalls. *See* Cisco ASA
- ASCII armoring, 42
- ASDM (Adaptive Security Device Manager), 113, 414–415, 423
- ASLR (address space layout randomization), 42
- ASNs (autonomous system numbers), 613
- ASRs (Aggregation Services Routers), 238
- assets, definition of, 12–13
- Assurance solution, Cisco DNA, 133, 135
- asymmetric algorithms, 84–86
- asymmetric key cryptography, 97
- AsyncOS, 642
- Attack Surface Management, 616–618
- attacks. *See* malware; threats
- attribute-based access control (ABAC), 179
- attribute/value pairs (AVPs), 187
- audits, cloud computing, 51, 607
- AUP (acceptable use policy), 642
- Aurora, 28
- authentication, 104. *See also* AAA (authentication, authorization, and accounting); management traffic security
 - 802.1X, 198, 334
 - 802.1AB*, 338–339
 - 802.1D*, 328–332
 - 802.1Q*, 323–326
 - 802.1w*, 332
 - Cisco ISE Identity Services*, 198, 334
 - configuration*, 213–222
 - monitor mode*, 306
 - RADIUS*, 213
 - roles in*, 188–190
- Active Directory (AD), 101, 653
- BeyondCorp, 169–171
- CAs (certificate authorities), 102–103
 - authenticating and enrolling with*, 91, 102–103
 - cross-certifying*, 106
 - hierarchical*, 105–106
 - single root*, 105
 - subordinate*, 105–106

- by characteristic, 164–165
- Cisco Secure Web Appliance, 653–655
- clientless remote-access VPNs, 546–548
- Duo Security, 166–168
- EAP (Extensible Authentication Protocol), 503, 519–520
- federated identity, 172, 174–177
- Flexible Authentication (Flex-Auth), 213
- JWT (JSON Web Token), 173–174
- key identification concepts, 162
- keychain, 404
- by knowledge, 162–164
- MAB (MAC Authentication Bypass), 196, 213, 302, 305, 402–404
- MD5, 87–88, 93, 400, 401–404, 497
- MD5 (Message Digest 5), 87–88, 93, 497
 - on BGP, 402–404*
 - on EIGRP, 401*
 - on OSPF, 400*
 - on RIP, 401–402*
- multifactor, 165, 357
- multilayer, 165, 357
- Open Authentication, 214
- by ownership or possession, 164
- passwordless, 175
- plaintext, 401
- pre-shared keys, 93, 497, 503
- RADIUS, 357–358
 - clientless remote-access VPNs in Cisco ASA, 547–548*
 - configuration, 213–215*
 - message exchange, 182–184*
 - TACACS+ versus, 185–186*
- router access, 357–358, 369–371
 - on BGP, 402–404*
 - on EIGRP, 401*
 - on OSPF, 400*
 - on RIP, 401–402*
- secure issuance, 162
- single-factor, 165, 357
- site-to-site VPNs, 530
- SSO (single sign-on), 171–173, 174–177
- TACACS+357–358
 - configuration, 207–212*
 - message exchange, 184*
 - RADIUS versus, 185–186*
- zero trust, 169–171
- authentication display legacy command, 214**
- authentication display new-style command, 214**
- Authentication Header (AH), 93, 500**
- authentication servers, 802.1X, 188–190**
- authentication-based vulnerabilities**
 - authentication attacks, 53
 - credential brute forcing, 34–35
 - default credentials, 35
 - Insecure Direct Object Reference vulnerabilities, 35–36
 - overview of, 33–34
 - password cracking, 34–35
 - session hijacking, 35
- authenticators, 189**
- authorization, 104. *See also* Cisco ISE (Identity Services Engine)**
 - attribute-based access control, 179
 - CoA (change of authorization), 204–207
 - custom privilege levels, 359, 371–373
 - discretionary access controls, 178
 - implicit deny, 177
 - mandatory access controls, 177
 - need to know, 161, 177
 - overview of, 177
 - parser views, 359, 374–375
 - RBAC (role-based access control), 178, 354–355, 359
- Auto NAT (Network Address Translation), 469**

auto secure utility, 345
 autoconfiguration, IPv6, 392
 autonomous system numbers (ASNs), 613
 availability, 46
 AVC (Application Visibility and Control),
 254–255, 257, 642, 655
 AVPs (attribute/value pairs), 187
 AWS (Amazon Web Services), 417, 590
 Azure, 417

B

backdoors, 19
 backlogs, 584
 Balanced Security and Connectivity
 policy, 474
 bandwidth management, 349
 BCPs (business continuity plans), 52, 608
 Beck, Ken, 586
 BeyondCorp, 169–171
 BFD (Bidirectional Forwarding
 Detection), 442
 BGP (Border Gateway Protocol),
 402–404, 468
 Bidirectional Forwarding Detection
 (BFD), 442
 BIKE, 95
 BinText, 28
 biometric systems, 164–165
 BIOS infection, 16
 black hat hackers, 14
 Black Hole Exploit Kit, 28
 BlackDuck Hub, 43
 blacklists, Cisco Secure Endpoint,
 681–682
 BLAKE2, 88, 93
 BLE (Bluetooth Low Energy), 56
 blind SQL injection, 33
 Block & Allow Lists, Cisco Secure
 Endpoint, 681–682

block ciphers, 84
 blocklisting, 483–484
 Blowfish, 84
 Bluetooth Low Energy (BLE), 56
 Bluetooth Smart, 56
 bootset security, 380–381
 Border Gateway Protocol (BGP),
 402–404, 468
 bot hosts/nets, 241, 414, 419
 BPDU Guard, 334, 335–336
 BPDUs (bridge protocol data units), 328
 bridge virtual interface (BVI), 438, 441
 bring-your-own-device (BYOD), 192
 browser vulnerabilities, 22
 brute-force attacks, 354
 buffer overflows, 41–42
 bugs, 392
 Build Applications with Cisco tutorial,
 140
 Build Database From Signature Set
 button (Cisco Secure Endpoint),
 680–681
 BVI (bridge virtual interface), 438, 441
 BYOD (bring-your-own-device), 192

C

C3PL (Cisco Common Classification
 Policy Language), 213, 214–215
 cables, console, 353–354
 cache
 cache poisoning, 341
 NetFlow, 240
 CAM (Content-Addressable Memory),
 336, 349, 390
 capability tables, 180–181
 Capability-Exchange-Answer (CEA), 187
 Capability-Exchange-Request (CER), 187
 capital expenditure (CapEx), 50

- CAPWAP (Control and Provisioning of Wireless Access Points), 257
- Carnegie Mellon University, SEI (Software Engineering Institute), 73
- CAs (certificate authorities), 98
 - authenticating and enrolling with, 91, 102–103
 - cross-certifying, 106
 - hierarchical, 105–106
 - single root, 105
 - subordinate, 105–106
- CASBs (cloud access security brokers), 643
- CASE (Cisco Context Adaptive Scanning Engine), 613
- cat Linux command, 86
- CBAC (Context-Based Access Control), 435
- CBWFQ (class-based weighted fair Queueing), 255
- CCNA Community, 700
- CD (continuous delivery), 583, 588–589
- CDO (Cisco Defense Orchestrator), 433–435
- CDP (Cisco Discovery Protocol), 338–339
- CEA (Capability-Exchange-Answer), 187
- CEF (Cisco Express Forwarding), 348
- cellular communication, 57
- CER (Capability-Exchange-Request), 187
- CER (crossover error rate), 165
- CERT Division, SEI (Software Engineering Institute), 74–75
- certificate authorities. *See* CAs (certificate authorities)
- certificate revocation list (CRL), 95
- certificate revocation lists (CRLs), 104
- certificates
 - digital
 - enrollment*, 91, 542–544
 - identity certificates*, 101
 - in practice*, 104–105
 - revoking*, 103–104
 - root certificates*, 99–100
 - identity, 101
 - root, 99–100
- Certification Roadmap, 699
- CERTs (Computer Emergency Response Teams), 74
- chain of custody, 61
- change of authorization (CoA), 204–207
- characteristic, authentication by, 164–165
- Check Point, 415–416
- Chrysler Comprehensive Compensation System (C3), 586
- CI (Concern Index), 273
- CI (continuous integration), 583, 588–589
- CIA triad, 43–46
- CIDR (classless interdomain routing), 682
- CIP (Common Industrial Protocol), 419
- cipher digit streams, 84
- ciphers
 - asymmetric algorithms, 84–86
 - block, 84
 - cryptographic, 34
 - definition of, 82–83
 - in IKE (Internet Key Exchange), 496
 - stream, 84
 - symmetric algorithms, 84–86
- ciphertext streams, 84
- CISA (Cybersecurity and Infrastructure Security Agency), 73
- Cisco ACI (Application Centric Infrastructure)
 - Cisco ACI Design Guide, 116
 - Cisco ISE (Identity Services Engine) integration, 310–312
 - micro-segmentation, 301
 - overview of, 114–116

- Cisco AMP (Advanced Malware Protection). *See* Cisco Secure Endpoint; Cisco Secure Malware Defense
- Cisco AnyConnect, 189, 261
- Cisco APIC (Application Policy Infrastructure Controller), 114–116
- Cisco ASA, 182
 - access control policies, 469–472
 - ACLs (access control lists), 452–458
 - application inspection, 458–459
 - Auto NAT (Network Address Translation), 469
 - client-based remote-access VPNs in
 - Cisco Secure Client*, 553–554
 - DTLS (Datagram Transport Layer Security)*, 555–556
 - overview of*, 551
 - split tunneling*, 554–555
 - tunnel and group policies*, 552–553
 - clientless remote-access VPNs in
 - application access*, 550–551
 - attributes and policy inheritance model*, 544
 - clientless SSL VPNs, enabling*, 548–549
 - design considerations*, 541–542
 - group policies*, 544–545
 - pre-SSL VPN configuration*, 542–544
 - SSL VPN modes*, 540–541
 - tunnel groups*, 545–546
 - user authentication*, 546–548
 - WebType ACLs*, 549–550
 - deployment modes, 437–448
 - features of, 414
 - FirePOWER module, 414–415
 - ICMP filtering in, 462–463
 - IPsec remote-access VPNs in, 538–540
 - NAT (Network Address Translation), 463–469
 - object grouping, 460–461
 - PAT (Port Address Translation), 463–469
 - site-to-site VPNs in, 537–538
 - advanced features*, 535–537
 - crypto maps*, 532–534
 - IPsec policy*, 531–532
 - ISAKMP, enabling*, 528–529
 - ISAKMP policy*, 529–530
 - NAT exempt policy*, 534–535
 - overview of*, 528–529
 - PFS (Perfect Forward Secrecy)*, 535
 - traffic filtering*, 534
 - tunnel groups*, 530–531
 - standard ACLs (access control lists), 461
 - through-the-box traffic filtering, 456
 - time-based ACLs (access control lists), 461–462
 - to-the-box traffic filtering, 459–460
 - WCCP (Web Cache Communication Protocol) configuration, 647–648
- Cisco ASAv (Adaptive Security Virtual Appliance), 414
- Cisco ASR 1000 Series Aggregation Service Routers (ASR 1000s), 254
- Cisco Async Operating System (AsyncOS), 642
- Cisco Attack Surface Management, 616–618
- Cisco AVC (Application Visibility and Control), 254–255, 257
- Cisco CASE (Context Adaptive Scanning Engine), 613
- Cisco Certification Roadmap, 699
- Cisco Cognitive Intelligence, 274–279
- Cisco Common Classification Policy Language (C3PL), 213, 214–215
- Cisco Content SMA (Security Management Appliance), 641–642, 662–667

- Cisco Defense Orchestrator (CDO), 433–435
- Cisco Discovery Protocol (CDP), 338–339
- Cisco DNA (Digital Network Architecture)
 - APIs (application programming interfaces), 135
 - Assurance solution, 133, 135
 - high-level architecture, 125–126
 - multivendor support, 136
 - network device APIs, 145
 - policies, 127–133
 - application*, 131–132
 - Cisco DNA Center Policy Overview dashboard*, 127–129
 - group-based access control*, 129
 - IP-based access control*, 131
 - traffic copy*, 132–133
 - Security solution, 135–136
- Cisco ETA (Encrypted Traffic Analytics), 135–136, 274
- Cisco Express Forwarding (CEF), 348
- Cisco FDM (Firepower Device Manager), 429–433
- Cisco Feature Navigator, 258
- Cisco Firepower intrusion policies
 - Cisco NGIPS preprocessors, 476–478
 - platform settings policy, 476
 - variables, 475–476
- Cisco Firewall Management Center, 648
- Cisco FTD (Firepower Threat Defense), 182, 415. *See also* Cisco Secure Firewall
 - access control policies in, 469–472
 - WCCP (Web Cache Communication Protocol) configuration, 648
- Cisco Guide to Harden Cisco IOS Devices, 389
- Cisco HyperFlex, 417
- Cisco IOS/IOS-XE
 - files, 362
 - NetFlow configuration, 280–294
 - configuration*, 286–293
 - flow exporters*, 286, 291–293
 - flow monitors*, 286, 289–291, 293–294
 - flow records*, 287–289
 - flow samplers*, 286
 - IPFIX export format*, 294
 - key fields*, 282–284
 - non-key fields*, 284–285
 - predefined records*, 285
 - records*, 282
 - simultaneous application tracking*, 281–282
 - user-defined records*, 286
 - site-to-site VPNs in, 506–508
- Cisco ISE Community Resources site, 312
- Cisco ISE (Identity Services Engine), 126, 549
 - accessing, 129
 - authorization rules, 198–199
 - benefits of, 192–193
 - Cisco Secure Network Analytics integration, 272
 - CoA (change of authorization), 204–207
 - context services, 195–198
 - deployment sizing, 224–225
 - design tips, 222–224
 - identity services, 198–199
 - network segmentation, 302–312
 - 802.1X/TrustSec in monitor mode*, 306
 - active policy enforcement*, 306–310
 - Cisco ACI integration*, 310–312
 - SGT assignment and deployment*, 306

- SXP (SGT Exchange Protocol)*, 303–305
 - posture assessment, 203–204
 - profiling services, 127, 195–198
- Cisco ISR (Integrated Services Routers), 254
- Cisco Meraki, 176, 268, 691–692
- Cisco NBAR2 (Network-Based Application Recognition Version 2), 132, 254–255
- Cisco NGIPSs (Next-Generation IPSs), 421–423, 476–478
- Cisco NVM (Network Visibility Module), 262
- Cisco NX-OS, 295–296, 362
- Cisco pxGrid (Platform Exchange Grid), 193–195
- Cisco QuantumFlow Processor, 258
- Cisco Resilient Configuration, 380–381
- Cisco routers, site-to-site VPNs in
 - DMVPN, 512–515
 - FlexVPN, 518–522
 - GETVPN, 512–518
 - GRE over IPsec, 508–510
 - multipoint GRE (mGRE) tunnels, 512
 - traditional site-to-site VPNs in Cisco IOS/Cisco IOS-XE, 506–508
 - troubleshooting, 522–528
 - tunnel interfaces, 506–508, 510–512
- Cisco SD-WAN (Software-Defined Wide Area Network), 569–573
- Cisco Secure Client, 189, 261, 504–505, 553–554
- Cisco Secure Cloud Analytics, 242, 263–268, 618–619
- Cisco Secure Cloud Insights. *See* Cisco Attack Surface Management
- Cisco Secure Email
 - Cisco SenderBase, 660–661
 - dashboards, 662–663
 - deployment, 659–660
 - DKIM (Domain Keys Identified Mail), 662
 - DLP (data loss prevention), 661
 - email encryption, 615
 - email protocols and concepts, 658–659
 - FED (Forged Email Detection), 614
 - listeners, 660
 - Malware Defense, 614
 - for Office 365, 615–616
 - overview of, 610–611, 641–642, 655–657, 658
 - RAT (recipient access table), 661
 - SMTP authentication and encryption, 661–662
 - SPF (Sender Policy Framework), 615
- Cisco Secure Endpoint, 237, 238
 - AMP Enabler, 688–689
 - connectors, 687
 - engines, 689
 - exclusion sets, 684–686
 - high-level architecture, 676–677
 - Outbreak Control
 - application control*, 683–684
 - custom detections*, 677–681
 - IP blacklists and whitelists*, 681–682
 - overview of, 675
 - policies, 687–688
 - reporting dashboards, 690–691
- Cisco Secure Firewall, 238, 414–415, 435
 - access control
 - access control policies*, 469–472
 - Auto NAT (Network Address Translation)*, 469
 - Cisco ASA ACLs (access control lists) in Cisco ASA*, 452–458
 - Cisco ASA application inspection*, 458–459

- Cisco ASA to-the-box traffic filtering*, 459–460
- ICMP filtering in Cisco ASA*, 462–463
- NAT (Network Address Translation)*, 463–469
- object grouping*, 460–461
- overview of*, 452
- PAT (Port Address Translation)*, 463–469
- standard ACLs (access control lists)*, 461
- time-based ACLs (access control lists)*, 461–462
- bot protection, 419
- CDO (Cisco Defense Orchestrator), 433–435
- Cisco ASA. *See* Cisco ASA
- Cisco Firepower intrusion policies
 - access control policies*, 472–475
 - Cisco NGIPS preprocessors*, 476–478
 - platform settings policy*, 476
 - variables*, 475–476
- Cisco Secure Malware Analytics, 479–483
- Cisco Secure Malware Defense
 - overview of*, 478–483
 - Security Intelligence blocklisting*, 483–484
 - Security Intelligence updates*, 484
- Cisco SecureX, 426–429
- Cloud Native solution, 417–418
- clustering, 450–452
- deployment modes, 415, 437–448
 - design considerations*, 447–448
 - interface modes*, 442–447
 - overview of*, 437
 - routed versus transparent*, 437–442
 - security contexts*, 438–439
- FDM (Firepower Device Manager), 429–433
- FMC (Firewall Management Center), 423–425
- high availability, 448–450
- history and legacy, 413–414
- interface modes, 442–444
 - inline pair*, 445
 - inline pair with tap*, 445–446
 - overview of*, 442–444
 - passive mode*, 446–447
 - passive with ERSPAN mode*, 447
- ISA3000, 418–419
- ISRs (Integrated Services Routers), 419–421
- Migration Tool, 415–416
- network security solutions, comparison of, 435–436
- NGIPS (Next-Generation IPS), 421–423
- overview of, 190–191, 413
- remote-access VPNs in, 557–566
 - overview of*, 556–557
 - Remote Access VPN Policy Wizard*, 557–566
 - troubleshooting*, 566–567
- SD-WAN (Software-Defined Wide Area Network), 419–421
- security zones, 431–432, 435
- site-to-site VPNs in, 567–569
- software updates, 484
- Threat Defense Virtual, 416–417
- WAFs (Web Application Firewalls), 419
- WCCP (Web Cache Communication Protocol) configuration, 648
- Zone-Based Firewall, 435
- Cisco Secure Malware Analytics, 30, 276, 479–483
- Cisco Secure Malware Defense, 674–675
 - overview of, 478–483

- Security Intelligence blocklisting, 483–484
- Security Intelligence updates, 484
- Cisco Secure Network Analytics. *See* network analytics
- Cisco Secure Web Appliance, 641–642
 - DLP (data loss prevention), 643, 655
 - explicit forward mode, 644–646
 - feature engines, 642–643
 - interface types, 644
 - overview of, 641–642
 - PBR (policy-based routing), 646, 651–652
 - policy configuration, 653–655
 - reports, 655–657
 - security services, 652
 - transparent mode, 646–647
 - WCCP (Web Cache Communication Protocol), 646–651
 - configuration in Cisco ASA, 647–648*
 - configuration on Cisco Secure Web Appliance, 650–651*
 - configuration on Cisco switches, 647–648*
 - definition of, 646*
 - transparent mode and, 646–647*
 - as web proxy, 643–644, 653
- Cisco Secure Workload, 622–626
 - ADM (Application Dependency Mapping), 622
 - agents, 622
 - definition of, 622
 - Forensics feature, 623
 - Security Dashboard, 623–626
- Cisco SecureX, 426–429
- Cisco SenderBase, 660–661
- Cisco Stealthwatch. *See* Cisco Secure Network Analytics
- Cisco Stealthwatch Cloud. *See* Cisco Secure Cloud Analytics
- Cisco switches, WCCP configuration on, 649–650
- Cisco Talos, 30, 264, 422, 472–473, 479, 484, 610–611, 614, 643
- Cisco TEA (ThousandEyes Enterprise Agent), 124–125
- Cisco TelePresence, 249
- Cisco Threat Response, 693
- Cisco TrustSec, 201–203, 306, 310–312
- Cisco UCS (Unified Computing System), 419
- Cisco Umbrella, 176
 - architecture, 609–610
 - Cisco Cognitive Intelligence integration, 276
 - Cisco Secure Cloud Analytics integration, 268
 - dashboard and reports, 611
 - Investigate, 610–611
 - overview of, 608–609
 - SIG (secure Internet gateway), 610–611
- Cisco vAnalytics, 571–573
- Cisco vManage, 571–573
- Cisco Webex, 176, 588
- Cisco WLCs (Wireless LAN Controllers), 254
- Cisco Workload Optimization Manager, 620
- Cisco XDR (eXtended Detection and Response), 627–632
- Cisco YANG Suite, 351–353
- Cisco-Maintained Exclusions, 684–686
- ClamAV, 479, 680
- class-based weighted fair Queueing (CBWFQ), 255
- Classic McEliece, 95
- classless interdomain routing (CIDR), 682
- class-map command, 459

- clear config crypto ikev2 policy command**, 530
- client-based remote-access VPNs**
 - Cisco Secure Client, 553–554
 - DTLS (Datagram Transport Layer Security), 555–556
 - overview of, 551
 - split tunneling, 554–555
 - tunnel and group policies, 552–553
- clientless remote-access VPNs (virtual private networks)**
 - application access, 550–551
 - attributes and policy inheritance model, 544
 - clientless SSL VPNs, enabling, 548–549
 - design considerations, 541–542
 - group policies, 544–545
 - pre-SSL VPN configuration, 542–544
 - SSL VPN modes, 540–541
 - tunnel groups, 545–546
 - user authentication, 546–548
 - WebType ACLs, 549–550
- clientless SSL VPNs (virtual private networks)**
 - application access, 550–551
 - enabling, 548–549
- cloud access security brokers (CASBs)**, 642
- cloud computing**
 - advantages of, 50
 - AppDynamics cloud monitoring, 619–622
 - CASBs (cloud access security brokers), 643
 - CD (continuous delivery), 583
 - characteristics of, 50
 - CI/CD pipelines, 583, 588–589
 - Cisco Attack Surface Management, 616–618
 - Cisco Secure Cloud Analytics, 242, 263–268, 618–619
 - Cisco Secure Email Threat Defense
 - email encryption*, 615
 - FED (Forged Email Detection)*, 614
 - for Office 365*, 615–616
 - overview of*, 612–613
 - SPF (Sender Policy Framework)*, 615
 - Cisco Secure Firewall Cloud Native, 417–418
 - Cisco Secure Workload, 622–626
 - ADM (Application Dependency Mapping)*, 622
 - agents*, 622
 - definition of*, 622
 - Forensics feature*, 623
 - Security Dashboard*, 623–626
 - Cisco Umbrella, 176
 - architecture*, 609–610
 - Cisco Cognitive Intelligence integration*, 276
 - Cisco Secure Cloud Analytics integration*, 268
 - dashboard and reports*, 611
 - Investigate*, 610–611, 612–613
 - overview of*, 608–609
 - SIG (secure Internet gateway)*, 610–611
 - Cisco XDR (eXtended Detection and Response), 627–632
- cloud security threats, 50–54
 - attacks*, 53
 - cloud computing models*, 50–52
 - security responsibilities*, 53–54
- cloud service models, 581–582
- cloud-based proxy, 610
- container orchestration
 - container images*, 592
 - Docker*, 592

- Kubernetes*, 597–602
 - overview of*, 592
- customer versus provider security
 - responsibility, 605–606
- definition of, 581–582
- DevOps, 583, 586–587
- DevSecOps, 603–605
- Malware Analytics Cloud
 - application control*, 683
 - Cisco Secure Endpoint*, 678
 - historical view of malware activity*, 677
 - IP blacklists and whitelists*, 680–681
- microservices and micro-segmentation, 602–603
- models for, 50
- patch management, 607
- security assessment, 607–608
- serverless, 589–591
- Cloud Native Firewall (CNFW), 417–418
- cloud service providers (CSPs), 605
- Cloud WAF (Web Application Firewall), 419
- cloud-based proxy, 610
- clusters, 17, 450–452
- CMZ (demilitarized zone), 643
- CNAs (CVE Naming Authorities), 10
- CNFW (Cloud Native Firewall), 417–418
- CoA (change of authorization), 204–207
- CoAP (Constrained Application Protocol), 57
- Cognitive Intelligence, 274–279
- cognitive threat analytics, Cisco Secure Web Appliance, 643
- collection considerations, NetFlow, 280
- collision resistance, 87
- command injection, 33
- command-line interface (CLI), 113
- commands. *See individual commands*
- Common Industrial Protocol (CIP), 419
- Common Object Request Broker Architecture (CORBA), 40, 140–141
- Common Security Advisory Framework (CSAF), 15
- Common Vulnerabilities and Exposures (CVE), 10, 31, 624
- Common Vulnerability Scoring System (CVSS), 69–73, 204
- communication, covert, 24–26
- community cloud, 582
- Compromise Event Types list, 690
- Computer Emergency Response Teams (CERTs), 74
- Computer Security Division (CSD), 7
- Concern Index (CI), 273
- Conficker, 28
- confidentiality, 12–13, 43–45
- configuration. *See also deployments*
 - AAA (authentication, authorization, and accounting). *See AAA (authentication, authorization, and accounting)*
 - Cisco ACI (Application Centric Infrastructure), 114–116
 - Cisco Secure Email
 - Cisco SenderBase*, 660–661
 - deployment*, 659–660
 - DKIM (Domain Keys Identified Mail)*, 662
 - DLP (data loss prevention)*, 661
 - email protocols and concepts*, 658–659
 - listeners*, 660
 - overview of*, 641–642, 655–657, 658
 - RAT (recipient access table)*, 661
 - SMTP authentication and encryption*, 661–662
 - Cisco Secure Web Appliance
 - explicit forward mode*, 644–646
 - interface types*, 644

- policies*, 653–655
- reports*, 655–657
- transparent mode*, 646–647
- WCCP (*Web Cache Communication Protocol*)
 - redirection*, 646–651
 - as web proxy*, 643–644
 - web proxy IP spoofing*, 653
- client-based remote-access VPNs in Cisco ASA
 - Cisco Secure Client*, 553–554
 - DTLS (Datagram Transport Layer Security)*, 555–556
 - overview of*, 551
 - split tunneling*, 554–555
 - tunnel and group policies*, 552–553
- clientless remote-access VPNs in Cisco ASA
 - application access*, 550–551
 - attributes and policy inheritance model*, 544
 - clientless SSL VPNs, enabling*, 548–549
 - design considerations*, 541–542
 - group policies*, 544–545
 - pre-SSL VPN configuration*, 542–544
 - SSL VPN modes*, 540–541
 - tunnel groups*, 545–546
 - user authentication*, 546–548
 - WebType ACLs*, 549–550
- clientless SSL VPNs
 - application access*, 550–551
 - enabling*, 548–549
- Docker images, 592–596
- IP blacklists and whitelists, 681–682
- IPsec remote-access VPNs in Cisco ASA, 538–540
- IPv6 security
 - ACLs (access control lists)*, 394–395
 - address format*, 383–384
 - address types*, 384–386
 - best practices*, 388–389, 393–394
 - IPv4 versus*, 381–382
 - moving to IPv6*, 388
 - risks*, 391–392
 - routing and routing protocols*, 386–388
 - security plans*, 388
 - threats*, 389–391
- Kubernetes, 598–602
- Layer 2 threat mitigation
 - best practices*, 333–334
 - BPDU Guard*, 335–336
 - CDP (Cisco Discovery Protocol)*, 338–339
 - DHCP snooping*, 339–341
 - dynamic ARP inspection*, 341–343
 - LLDP (Link Layer Discovery Protocol)*, 338–339
 - negotiations, preventing*, 334
 - overview of*, 334–335
 - port security*, 336–338
 - Root Guard*, 336
- logging, 360–361, 378–379
- management traffic security
 - best practices*, 354–356
 - Cisco IOS and Cisco NX-OS files*, 362
 - console cable*, 353–354
 - definition of*, 350
 - NETCONF (Network Configuration Protocol)*, 350–353
 - NTP (Network Time Protocol)*, 379–380
 - NTP (Network Time Protocol), overview of*, 361

- password recommendations*, 354, 356–357, 362–364
- RESTCONF (*RESTful Network Configuration Protocol*), 350–353
- SNMP (*Simple Network Management Protocol*), 350–353
- user authentication*, 354, 357
- NetFlow. *See* NetFlow
- remote-access VPNs in Cisco Secure Firewall
 - overview of*, 556–557
 - Remote Access VPN Policy Wizard*, 557–566
 - troubleshooting*, 566–567
- site-to-site VPNs in Cisco ASA, 537–538
 - advanced features*, 535–537
 - crypto maps*, 532–534
 - IPsec policy*, 531–532
 - ISAKMP, enabling*, 528–529
 - ISAKMP policy*, 529–530
 - NAT exempt policy*, 534–535
 - overview of*, 528–529
 - PFS (Perfect Forward Secrecy)*, 535
 - traffic filtering*, 534
 - tunnel groups*, 530–531
- site-to-site VPNs in Cisco routers
 - DMVPN*, 512–515
 - FlexVPN*, 518–522
 - GETVPN*, 512–518
 - GRE over IPsec*, 508–510
 - multipoint GRE (mGRE) tunnels*, 512
 - traditional site-to-site VPNs in Cisco IOS/Cisco IOS-XE*, 506–508
 - troubleshooting*, 522–528
 - tunnel interfaces*, 506–508, 510–512
- site-to-site VPNs in Cisco Secure Firewall, 567–569
- vulnerabilities in, 9
- WCCP (*Web Cache Communication Protocol*)
 - in Cisco ASA*, 647–648
 - on Cisco Secure Web Appliance*, 650–651
 - on Cisco switches*, 649–650
- configure terminal command**, 290
- CONNECT method**, 139
- Connectivity Over Security policy**, 474
- connectors**
 - Cisco Secure Endpoint, 687
 - Cisco Secure Workload, 624
- console cable**, 353–354
- constant special ID lists (CSIDL)**, 685
- Constrained Application Protocol (CoAP)**, 57
- consumers, Cisco Secure Workload**, 624
- container orchestration**
 - container images, 592
 - Docker, 592
 - Kubernetes, 597–602
 - overview of, 592
- container registries**, 592
- content security**
 - AsyncOS, 642
 - Cisco Content SMA (*Security Management Appliance*), 641–642, 662–667
 - Cisco Secure Email
 - Cisco SenderBase*, 660–661
 - dashboards*, 662–663
 - deployment*, 659–660
 - DLP (data loss prevention)*, 661
 - email protocols and concepts*, 658–659
 - listeners*, 660
 - overview of*, 641–642, 658
 - RAT (recipient access table)*, 661

- SMTP authentication and encryption*, 661–662
- Cisco Secure Web Appliance, 642
 - DLP (data loss prevention)*, 643, 655
 - explicit forward mode*, 644–646
 - feature engines*, 642–643
 - interface types*, 644
 - overview of*, 641–642
 - PBR (policy-based routing)*, 646, 651–652
 - policy configuration*, 653–655
 - reports*, 655–657
 - security services*, 652
 - transparent mode*, 646–647
 - WCCP (Web Cache Communication Protocol)*, 646–651
 - as web proxy*, 643–644, 653
- overview of, 641–642
- Content-Addressable Memory (CAM), 336, 349, 390
- content-dependent access control, 182
- context services, Cisco ISE (Identity Services Engine), 195–198
- Context-Based Access Control (CBAC), 435
- continuous delivery (CD), 583
- continuous integration (CI), 583, 588–589
- Contiv, 120, 123–124, 602–603
- contracts, Cisco DNA (Digital Network Architecture), 129
- Control And Provisioning of Wireless Access Points (CAPWAP), 257
- Control Plane Policing (CoPP), 347, 397–399
- Control Plane Protection (CPPr), 348, 399
- control plane security, 113
 - best practices, 347–348
 - CoPP (Control Plane Policing), 347, 397–399
 - CPPr (Control Plane Protection), 348, 399
 - overview of, 344–345, 395
 - process-switched traffic, 395–397
 - routing protocols, 399–400
 - on BGP*, 402–404
 - on EIGRP*, 401
 - on OSPF*, 400
 - on RIP*, 401–402
- controllers, SDN (software-defined networking), 114
- control-plane keyword, 460
- co-occurrence model, 610
- cookies
 - Cisco Secure Web Appliance, 654
 - cookie manipulation attacks, 39
- coordination centers, 74–75
- CoPP (Control Plane Policing), 347, 397–399
- CORBA (Common Object Request Broker Architecture), 40, 140–141
- corp-net SSID, 131
- covert channels, 25
- covert communication, 24–26
- CPPr (Control Plane Protection), 348, 399
- Create IP List button (Cisco Secure Endpoint), 682
- create_deck() function, 144
- credential brute forcing, 34–35
- credentials, default, 35
- CRLs (certificate revocation lists), 95, 104
- cross-certification, 106
- crossover error rate (CER), 165
- cross-site request forgery (CSRF), 38
- cross-site scripting (XSS), 33, 36–38, 53
- cryptanalysis, 82

- Cryptcat, 26
- crypters, 23
- crypto ca authenticate command, 542
- crypto ca import command, 543
- crypto ikev1 enable outside command, 529
- crypto maps, 506
 - IPsec remote-access VPNs in Cisco ASA, 539
 - site-to-site VPNs in Cisco ASA firewalls, 532–534
- cryptocurrency wallets, 20
- Cryptographic Suite for Algebraic Lattices (CRYSTALS), 94
- cryptography
 - cipher digit streams, 84
 - ciphers
 - asymmetric algorithms*, 84–86
 - block*, 84
 - cryptographic*, 34
 - definition of*, 82–83
 - in IKE (Internet Key Exchange)*, 496
 - stream*, 84
 - symmetric algorithms*, 84–86
 - ciphertext streams, 84
 - CyberChef, 89
 - definition of, 82
 - hashes
 - AES-256*, 89
 - BLAKE2*, 88, 93
 - example of*, 86–87
 - HMAC*, 89
 - MD5*, 87–88, 93, 400–404, 497
 - SHA*, 93
 - SHA-1*, 88
 - SHA-2*, 88
 - SHA-3*, 88
 - SHA-256*, 678–680
 - SHA-384*, 89
 - SHA512 checksum*, 86
 - Whirlpool*, 88, 93
- IPsec, 93
 - key management, 83–84, 92
 - NGE (next-generation encryption), 92–93
 - PKI (public key infrastructure)
 - asymmetric key cryptography*, 97
 - CAs (certificate authorities)*, 91, 98, 102–106
 - definition of*, 97
 - digital certificates*, 103–105
 - digital signatures*, 90–91, 97–98, 503
 - identity certificate*, 101
 - PGP (Pretty Good Privacy)*, 97
 - public and private key pairs*, 85, 97, 98
 - public key cryptography*, 97
 - root certificates*, 99–100
 - standards*, 103
 - topologies*, 105–106
 - X.500*, 101–102
 - X.509v3*, 101–102
 - post-quantum, 93–95
 - SSL (Secure Sockets Layer), 95–96
 - symmetric algorithms, 84–86
 - TLS (Transport Layer Security), 95–96
- cryptology, 82
- CRYSTALS (Cryptographic Suite for Algebraic Lattices), 94
- CSAF (Common Security Advisory Framework), 15
- CSD (Computer Security Division), 7
- CSIDL (constant special ID lists), 685
- CSIRTs (computer security incident response teams), 67–69, 74
- CSPs (cloud service providers), 605
- CSRF (cross-site request forgery), 38

- cts role-based enforcement command, 306
- cts role-based enforcement vlan-list command, 306
- curl command, 141–143
- custom detections, Cisco Secure Endpoint Outbreak Control, 677–681
- custom feeds, 484
- custom privilege levels, 359, 371–373
- customer security responsibility, cloud computing, 605–606
- CVE (Common Vulnerabilities and Exposures), 10, 31
- CVE Naming Authorities (CNAs), 10
- CVSS (Common Vulnerability Scoring System), 69–73, 204, 624
- CyberChef, 89
- cybersecurity
 - information security versus, 6–7
 - overview of, 6
 - standards, 7–8
- Cybersecurity and Infrastructure Security Agency (CISA), 73

D

- DAC (Dynamic Authorization Client), 205
- dACLs (downloadable access control lists), 191
- DACs (discretionary access controls), 49, 178
- DAI (dynamic ARP inspection), 334, 341–343, 349, 390
- dark web, 10
- DAS (Dynamic Authorization Server), 205
- dashboards
 - Cisco DNA (Digital Network Architecture), 127–129
 - Cisco Secure Cloud Analytics, 242
 - Cisco Secure Email, 662–663
 - Cisco Secure Endpoint, 690–691
 - Cisco Secure Network Analytics, 268–270
 - Cisco Secure Workload, 623–626
 - Cisco Umbrella, 611
 - Cognitive Intelligence, 274–279
- DAST (dynamic application security testing), 604–605
- Data Center Network Manager (DCNM), 124
- data centers, NetFlow deployment on, 259–261
- data classification, cloud computing, 52
- Data Distribution Protocol (DDP), 57
- data leak detection and prevention, NetFlow, 243
- data loss prevention (DLP)
 - Cisco Secure Email, 661
 - Cisco Secure Web Appliance, 643, 655
- data plane security, 113
 - best practices, 348–349
 - in IPv6
 - ACLs (*access control lists*), 394–395
 - best practices*, 388–389, 393–394
 - focus on*, 390–391
 - IPv4 versus*, 381–382
 - IPv6 address format*, 383–384
 - IPv6 address types*, 384–386
 - moving to IPv6*, 388
 - risks*, 391–392
 - routing and routing protocols*, 386–388
 - security plans*, 388
 - threats*, 389–390
 - overview of, 344–345
- data-driven segmentation, 297–299
- Datagram Transport Layer Security (DTLS), 555–556, 566

- data-hiding Trojans, 19
- DCE/RPC preprocessor, 476
- DCNM (Data Center Network Manager), 124
- DCOM (Distributed Component Object Model), 40, 140–141
- DDoS (distributed denial-of-service) attacks, 13, 53, 241–243
- DDP (Data Distribution Protocol), 57
- Dead Peer Detection (DPD), 501
- debug aaa accounting command, 369–371
- debug aaa authentication command, 369–371
- debug aaa authorization command, 369–371
- debug crypto ikev2 command, 525–527
- debug crypto ikev2 internal command, 525–527
- debug crypto ipsec command, 525–527
- debug crypto isakmp command, 525–527
- debug feature command, 566
- debug radius authentication command, 525–527
- debug webvpn condition command, 566
- debugging. *See also* troubleshooting
 - AAA (authentication, authorization, and accounting), 369–371
 - site-to-site VPNs in Cisco routers, 522–528
 - TACACS+210–212
- Deck of Cards API, 141–144
- deep packet inspection (DPI), 254, 420
- deep web, 10
- default allow, 48
- default credentials, 35
- default deny, 48
- default gateways, site-to-site VPNs, 536
- DELAY quarantine, 661
- DELETE method, 139
- demilitarized zone (DMZ), 643
- denial-of-service attacks. *See* DoS (denial-of-service) attacks
- Department of Homeland Security (DHS), 74
- deployments. *See also* configuration
 - Cisco Secure Firewall, 437–448
 - design considerations*, 447–448
 - interface modes*, 442–447
 - overview of*, 437
 - routed versus transparent*, 437–442
 - security contexts*, 438–439
 - Kubernetes, 598–602
 - NetFlow, 255–262
 - data center*, 259–261
 - Internet edge*, 258–259
 - site-to-site and remote VPNs*, 261–262
 - user access layer*, 256
 - wireless LAN*, 256–257
- DES (Digital Encryption Standard), 84, 93, 496
- design considerations
 - Cisco ISE (Identity Services Engine), 222–224
 - clientless remote-access VPNs in Cisco ASA, 541–542
- designated ports, 331
- destination command, 291
- destination SGT (DGT), 202
- development methodologies
 - Agile, 583–586
 - Scrum, 584–585
 - waterfall, 583
- device flow correlation (DFC), 681
- device hardening, 389
- device image security, 380–381
- Device-Watchdog-Answer (DWA), 187
- Device-Watchdog-Request (DWR), 187

- DevNet, 135, 140
- DevNet ACI Programmability tutorial, 140
- DevNet Developer Videos tutorial, 140
- DevNet Git Tutorials tutorial, 140
- DevNet GitHub Repositories tutorial, 140
- DevOps, 583, 586–587
- DevSecOps, 603–605
- DFC (device flow correlation), 681
- DFIR (digital forensics and incident response)
 - EDR (Endpoint Detection and Response), 676
 - false positives/false negatives, 60
 - incident response
 - CERTs (Computer Emergency Response Teams)*, 74
 - coordination centers*, 74–75
 - CSIRTs (computer security incident response teams)*, 67–69, 74
 - CVSS (Common Vulnerability Scoring System)*, 69–73
 - definition of*, 62
 - forensic evidence*, 61–62
 - incident response process*, 63–65
 - information sharing and coordination*, 66
 - IRPs (incident response plans)*, 62–63
 - key incident management personnel*, 75–76
 - PSIRTs (product security incident response teams)*, 69
 - SSVC (Stakeholder-Specific Vulnerability Categorization)*, 73
 - tabletop exercises and playbooks*, 65–66
- incidents
 - examples of*, 59–60
 - reporting*, 61–62
 - severity levels*, 60
- ISO/IEC 27002:2013, 58–59
- NIST (National Institute of Standards and Technology) guidelines for, 58–59
 - true positives/true negatives, 60
- DGT (destination SGT), 202
- DH. *See* Diffie-Hellman (DH)
- DHCP (Dynamic Host Configuration Protocol), 385, 414, 437
 - DHCP snooping, 334, 339–341, 349
 - DHCPv6, 391
- DHS (Department of Homeland Security), 74
- Diameter, 186–188
- dictionary attack, 354
- differentiated services code point (DSCP), 239
- Diffie-Hellman (DH), 86, 93
 - IKEv1 Phase 1 negotiation, 496–498
 - IKEv1 Phase 2 negotiation, 499
 - IKEv2, 530
 - PFS (Perfect Forward Secrecy), 535
- dig command, 658
- digest, 87
- digital certificates
 - enrollment, 91, 542–544
 - identity certificates, 101
 - in practice, 104–105
 - revoking, 103–104
 - root certificates, 99–100
- Digital Encryption Standard (DES), 84, 496
- digital forensics and incident response. *See* DFIR (digital forensics and incident response)
- Digital Network Architecture. *See* Cisco DNA (Digital Network Architecture)

- Digital Signature Algorithm (DSA), 86, 93
- digital signatures, 90–91, 97–98, 503
- Dilithium, 94
- disaster recovery, cloud computing, 52
- Disconnect-Peer-Answer (DPA), 187
- Disconnect-Peer-Request (DPR), 187
- Disconnect-Request, 206
- discretionary access controls (DACs), 49, 178
- Distributed Component Object Model (DCOM), 40, 140–141
- distributed denial-of-service attacks. *See* DDoS (distributed denial-of-service) attacks
- Distributed Network Protocol (DNP3), 418
- distribution of malware, 22–23
- DKIM (Domain Keys Identified Mail), 615, 662
- DLP (data loss prevention)
 - Cisco Secure Email, 661
 - Cisco Secure Web Appliance, 643, 655
- DLP Incident Summary dashboard, Cisco Secure Email, 667
- DMARC (Domain-based Message Authentication, Reporting, and Conformance), 615
- DMVPN (Dynamic Multipoint VPN), 262, 498, 512–515
- DNA (Digital Network Architecture). *See* Cisco DNA (Digital Network Architecture)
- DNP3 (Distributed Network Protocol), 418
- DNS (Domain Name System)
 - covert communication, 25–26
 - DNS attacks, 53
 - DNS preprocessor, 476
- Docker, 592
- docker images command, 593, 596
- docker ps command, 594
- docker run mypython command, 596
- docker search command, 594
- Docker Swarm, 123, 592
- Dockerfiles, 595–596
- Document Object Model (DOM), 37
- documentation
 - APIs (application programming interfaces), 141
 - Docker, 597
 - ISO (International Organization for Standardization), 8
- DOM (Document Object Model), 37
- domain and IP reputation scores, 613
- domain co-occurrences, 613
- Domain Keys Identified Mail (DKIM), 662
- Domain Name System. *See* DNS (Domain Name System)
- Domain-based Message Authentication, Reporting, and Conformance (DMARC), 615
- DomainKeys Identified Mail (DKIM), 615
- DoS (denial-of-service) attacks, 13, 19, 46–48, 389–390, 502
- downloadable access control lists (dACLs), 191
- downloading
 - Cisco Secure Endpoint connectors, 687
 - Contiv, 123, 602
- DPA (Disconnect-Peer-Answer), 187
- DPD (Dead Peer Detection), 501
- DPI (deep packet inspection), 254, 420
- DPR (Disconnect-Peer-Request), 187
- DR/BCP (disaster recovery/business continuity plan), 52, 608
- droppers, 23, 27
- DSA (Digital Signature Algorithm), 86
- DSCPs (differentiated services code points), 239

DTLS (Datagram Transport Layer Security), 555–556, 566

dual stacks, 392

due diligence, 52, 608

Duo Security, 166–168, 357

duties, separation of, 161

dVTI (dynamic VTI), 512

DWA (Device-Watchdog-Answer), 187

DWR (Device-Watchdog-Request), 187

dynamic analysis, malware, 29–30

dynamic application security testing (DAST), 604–605

dynamic ARP inspection (DAI), 334, 341–343, 349, 390

Dynamic Authorization Client (DAC), 205

Dynamic Authorization Server (DAS), 205

Dynamic Host Configuration Protocol (DHCP), 385, 414, 437

Dynamic Multipoint VPN (DMVPN), 262, 498, 512–515

dynamic NAT (Network Address Translation), 463–469

dynamic tunnel interfaces, 511–512

dynamic VTI (VTI), 512

E

EAP (Extensible Authentication Protocol), 189, 503, 519–520

EAP-Identity-Request, 213

EAPoL (EAP over LAN), 189–190, 213

East-West traffic, 118, 259

eavesdropping, 390

e-banking Trojans, 19

ECC (Elliptic Curve Cryptography), 86, 93

ECDSA algorithm, 93

ECMP (equal-cost multi-path routing), 117

EDR (Endpoint Detection and Response), 676

EEPGs (External Endpoint Groups), 310

EER (equal error rate), 165

EIGRP (Enhanced Interior Gateway Routing Protocol), 248, 347, 401, 414

Elastic Kubernetes Service (EKS), 417

Elastic Search, 246

electrostatic discharge (ESD), 62

ElGamal, 86

ELK stack, 246

Elliptic Curve Cryptography (ECC), 86, 93

email

- Cisco Secure Email
 - Cisco SenderBase*, 660–661
 - dashboards*, 662–663
 - deployment*, 659–660
 - DKIM (Domain Keys Identified Mail)*, 662
 - DLP (data loss prevention)*, 661
 - email protocols and concepts*, 658–659
 - listeners*, 660
 - overview of*, 641–642, 658
 - RAT (recipient access table)*, 661
 - SMTP authentication and encryption*, 661–662
- Cisco Secure Email Threat Defense
 - email encryption*, 615
 - FED (Forged Email Detection)*, 614
 - for Office 365*, 615–616
 - overview of*, 610–611
 - SPF (Sender Policy Framework)*, 615
 - Trojan infection on, 21

enable command, 289, 359

- enable password command, 358
- Encapsulated Remote Switched Port Analyzer (ERSPAN), 132
- Encapsulating Security Payload (ESP), 93, 447, 500, 536
- enclave networks, 296
- encrypted management protocols, 355, 359–360, 375–378
- Encrypted Traffic Analytics (ETA), 135–136, 274
- encryption. *See* cryptography
- end command, 290
- endpoint (EP) configuration, 310
- Endpoint Detection and Response (EDR), 676
- endpoint groups (EPGs), 301
- endpoint protection and detection
 - Cisco Secure Endpoint
 - AMP Enabler*, 688–689
 - connectors*, 687
 - engines*, 689
 - exclusion sets*, 684–686
 - high-level architecture*, 676–677
 - Outbreak Control*, 677–683
 - overview of*, 675
 - policies*, 687–688
 - reporting dashboards*, 690–691
 - Cisco Secure Firewall Malware Defense, 674–675
 - Cisco Threat Response, 693
 - EDR (Endpoint Detection and Response), 676
 - EPP (Endpoint Protection Platform), 676
 - ETDR (Endpoint Threat Detection and Response), 676
- Endpoint Protection Platform (EPP), 676
- Endpoint Threat Detection and Response (ETDR), 676
- endpoints
 - PTEP (physical tunnel endpoint), 114
 - VTEP (VXLAN tunnel endpoint), 114
- enforcers, networks as, 238
- engines, Cisco Secure Endpoint, 689
- Enhanced Interior Gateway Routing Protocol (EIGRP), 248, 347, 401, 414
- enhanced local mode, NetFlow, 257
- enrollment terminal subcommand, 543
- environment-data download, 305
- EP (endpoint) configuration, 310
- EP (Extreme Programming), 586
- EPGs (endpoint groups), 301
- EPP (Endpoint Protection Platform), 676
- equal error rate (EER), 165
- equal-cost multi-path routing (ECMP), 117
- ERSPAN (Encapsulated Remote SPAN), 132, 447
- ESD (electrostatic discharge), 62
- ESP (Encapsulating Security Payload), 93, 447, 500, 536
- ETA (Encrypted Traffic Analytics), 135–136, 274
- ETDR (Endpoint Threat Detection and Response), 676
- EtherType ACLs (access control lists), 456
- ethical hackers, 13–14
- Ethos, 480–481, 689
- ETSI (European Telecommunications Standards Institute), 123
- Evan's Debugger (edb), 28
- evasion techniques, IDSs (intrusion detection systems), 60
- events, definition of, 59
- evidence, forensic, 61–62
- exam, SCOR 350–701
 - exam updates, 698–700
 - final review and study, 696–697
 - hand-on preparation activities, 696
 - Pearson Test Prep software, 697

exclusion sets, Cisco Secure Endpoint, 684–686
 EXEC shell, 357–358
 explicit forward mode, Cisco Secure Web Appliance, 644–646
 Exploit Database, 10
 exploits
 definition of, 10–11
 zero-day, 10
 export-protocol command, 291
 export-protocol ipfix command, 294
 extended ACLs (access control lists), 455
 eXtended Detection and Response (XDR), 426–427, 618, 627–632
 Extensible Access Control Markup Language (XACML), 179
 Extensible Authentication Protocol (EAP), 189, 503, 519–520
 Extensible Messaging and Presence Protocol (XMPP), 57, 193
 Extension exclusion type, 684
 External Endpoint Groups (EEPGs), 310
 Extreme Programming (EP), 586

F

Facebook Connect, 172
 factors, 165
 failover, Cisco Secure Firewall, 448–450
 FakeNet, 29–30
 false acceptance errors (FAR), 165
 false positives/false negatives, 60
 false rejection errors (FRR), 165
 FAR (false acceptance errors), 165
 Faraday cage, 62
 fast flux, 610
 fast infection, 17
 FCM (FXOS Firepower Chassis Manager), 432
 FDM (Firepower Device Manager), 429–433
 feature netflow command, 295
 FED (Forged Email Detection), 614
 Federal Information Processing Standards (FIPS), 7
 Federal Information Security Management Act (FISMA), 59
 Federally Funded Research and Development Center (FFRDC), 10
 federated identity, 174–177
 federation providers, 174
 feedback loop, DevOps, 587
 FFRDC (Federally Funded Research and Development Center), 10
 file infection, 16
 file reputation, 643, 675
 file retrospection, 478–483, 643, 666, 675
 file sandboxing, 478–483, 643, 675
 File Transfer Protocol (FTP), 476, 647–648, 650
 Filter-ID, 205
 filtering
 EDR (Endpoint Detection and Response), 676
 ports, 399
 Financial Services Information Sharing and Analysis Center (FS-ISAC), 66
 Findsecbugs, 604
 FIPS (Federal Information Processing Standards), 7
 FireAMP. *See* Cisco Secure Endpoint
 Firepower Device Manager (FDM), 429–433
 Firepower eXtensible Operating System (FXOS), 432
 Firepower Management Center. *See* FMC (Firewall Management Center)
 FirePOWER module, 414–415

- Firepower Threat Defense (FTD), 182, 415, 648. *See also* Cisco Secure Firewall
- Firewall Management Center (FMC), 414–415, 423–425
- firewalls, 349
- FIRST website, 72
- five-tuple, 238–239
- Flame, 17
- FlexConfig objects, 648
- Flexible Authentication (Flex-Auth), 213
- Flexible NetFlow, 280–294
 - configuration, 286–293
 - flow exporters, 286, 291–293, 295
 - flow monitors, 286, 289–291, 293–294, 295–296
 - flow samplers, 286
 - IPFIX export format, 294
 - key fields, 282–284
 - non-key fields, 284–285
 - records, 282
 - flow records*, 287–289, 295
 - predefined records*, 285
 - user-defined records*, 286
 - simultaneous application tracking, 281–282
- FlexNet Code Insight, 43
- FlexVPN, 262, 511, 518–522
- flow, definition of, 238–241
- flow anomaly detection, 305
- flow de-duplication, 305
- flow exporter command, 291
- flow exporters, 286, 291–293, 295
- flow licenses, 264
- flow monitor command, 290
- flow monitors, 286, 289–291, 293–294, 295–296
- Flow Observation, 624
- flow records, 287–289, 295
- flow samplers, 286
- Flow Search page, Cisco Secure Workload, 624
- flow stitching, 305
- FlowCollector, 263
- FlowReplicator, 264
- flows per second, 279–280
- FlowSensors, 238, 246, 260–261, 264
- FMC (Firewall Management Center), 414–415, 423–425
- fog computing, 54–56
- Forensics, Cisco Secure Workload, 623–626
- Forensics Scores, 623
- forests, 174
- Forged Email Detection (FED), 614
- Fortinet, 415–416
- FQDNs (fully qualified domain names), 98
- fragmentation, 60, 396, 536
- frames, VXLAN (Virtual Extensible LAN), 116–117
- freeware, Trojan infection on, 22
- FRR (false rejection errors), 165
- FS-ISAC (Financial Services Information Sharing and Analysis Center), 66
- FTD (Firepower Threat Defense), 182, 415, 648. *See also* Cisco Secure Firewall
- FTP (File Transfer Protocol), 476, 647–648, 650
- full tunnel client mode, 540–541
- fully qualified domain names (FQDNs), 98
- fuzzing, 604–605
- FXOS (Firepower eXtensible Operating System), 432
- FXOS Firepower Chassis Manager (FCM), 432

G

- Galois/Counter Mode (GCM), 93
- GCKS (group controller or key server), 516
- GCM (Galois/Counter Mode), 93
- GCP. *See* Google Cloud Platform (GCP)
- GDOI (Group Domain of Interpretation), 515–516
- General Packet Radio Service (GPRS), 477
- Generic Network Virtualization Encapsulation (GENEVE), 116
- Generic Routing Encapsulation. *See* GRE (Generic Routing Encapsulation)
- GENEVE (Generic Network Virtualization Encapsulation), 116
- geolocation, 484, 613, 614
- GET method, 139
- GETVPN (Group Encrypted Transport VPN), 512–518
- Ghidra, 28
- GitHub, 10
- GKE (Google Kubernetes Engine), 599
- gNMI (gRPC Network Management Interface), 151, 352–353
- Go, 137
- Google Cloud Platform (GCP), 417
 - GKE (Google Kubernetes Engine), 599
 - GPC Flow Logs, 265
- Google Kubernetes Engine (GKE), 599
- government threat actors, 13
- GPOs (Group Policy Objects), 645
- GPRS (General Packet Radio Service), 477
- graphical user interfaces (GUIs), 113
- GraphQL, 40, 141
- gray hat hackers, 14
- Graylog, 246
- GRE (Generic Routing Encapsulation), 262, 494
 - Diffie-Hellman, 511
 - GRE over IPsec, 508–510, 511
 - multipoint GRE (mGRE) tunnels, 512
- group controller or key server (GCKS), 516
- Group Domain of Interpretation (GDOI), 515–516
- Group Encrypted Transport VPN (GETVPN), 512–518
 - group policies, 129, 544–545
- Group Policy Objects (GPOs), 645
- groups, Cisco Secure Endpoint, 687
- gRPC Network Management Interface (gNMI), 151, 352–353
- GTP (GPRS Tunneling Protocol), 477
- guest networks, 297
- GUIs (graphical user interfaces), 113

H

- hackerrepo.org repository, 16
- hackers, 13
- hacktivists, 13
- hands-on exam preparation activities, 696
- hardening, device, 389
- hardware vulnerabilities. *See* vulnerabilities
- HashCorp Nomad, 592
- Hashed Message Authentication Code (HMAC), 89
- hashes, 530
 - AES-256, 89
 - BLAKE2, 88, 93
 - example of, 86–87
 - group policies, 87–88
 - HMAC, 89
 - MD5, 87–88, 93, 497

- on BGP, 402–404*
 - on EIGRP, 401*
 - on OSPF, 400*
 - on RIP, 401–402*
 - SHA, 93
 - SHA-1, 88
 - SHA-2, 88
 - SHA-3, 88
 - SHA-256, 678–680
 - SHA-384, 89
 - SHA512 checksum, 86
 - Whirlpool, 88, 93
 - HEAD method, 139
 - hierarchical CAs (certificate authorities), 105–106
 - hierarchical PKI topology, 105
 - high availability, 448–450
 - high-level architecture, Cisco Secure Endpoint, 676–677
 - hijacking, session, 35, 53
 - HMAC (Hashed Message Authentication Code), 89
 - hop-by-hop extension headers, 391–392
 - Horizon, 120
 - host sub-interface, 348
 - HQC, 95
 - HTML injection, 33
 - HTTP (Hypertext Transfer Protocol)
 - Cisco Secure Web Appliance traffic redirection, 647–648, 650
 - HTTP preprocessor, 476
 - methods, 139
 - status codes, 139
 - HTTPS (HTTP Secure), 104, 355
 - Cisco Secure Endpoint, 677
 - HTTPS proxy, 655
 - for IPv4/IPv6, 389
 - SSL (Secure Sockets Layer) VPNs, 95, 504
 - hub-and-spokes configuration, DMVPN, 514–515
 - hybrid cloud, 582
 - HyperFlex, 417
-
- IaaS (Infrastructure as a Service)
 - customer versus provider security responsibility, 605–606
 - definition of, 50–51, 582
 - ICMP (Internet Control Message Protocol), 25–26, 349, 395, 462–463
 - icmp command, 462
 - ICMPv6, 392
 - IDA Pro, 28
 - IDE (intrusion detection systems), 420
 - IDEA (International Data Encryption Algorithm), 84
 - identification, 162
 - identity certificate, 101
 - identity providers (IdPs), 174
 - Identity Services Engine. *See* Cisco ISE (Identity Services Engine)
 - IDLs (interface description languages), 151
 - IdPs (identity providers), 174
 - IDSs (intrusion detection systems), 420, 472
 - IEC61850, 419
 - IEPGs (Internal Endpoint Groups), 310
 - IKE (Internet Key Exchange), 93
 - IKEv1 Phase 1 negotiation, 496–498
 - IKEv1 Phase 2 negotiation, 498–501
 - IKEv2, 501–503
 - IM (instant messaging), Trojan infection on, 21
 - images, container, 592
 - IMAP (Internet Message Access Protocol), 477, 658

ImmUNET AV, 479

impersonated mobile apps, 22

implicit deny, 177

in-band management, 356

in-band SQL injection, 33

incident response

- CERTs (Computer Emergency Response Teams), 74
- coordination centers, 74–75
- CSIRTs (computer security incident response teams), 67–69, 74
- CVSS (Common Vulnerability Scoring System), 69–73
- definition of, 62
- forensic evidence, 61–62
- incident response process, 63–65
- information sharing and coordination, 66
- IRPs (incident response plans), 62–63
- key incident management personnel, 75–76
- NetFlow, 243–248
- PSIRTs (product security incident response teams), 69
- SSVC (Stakeholder-Specific Vulnerability Categorization), 73
- tabletop exercises and playbooks, 65–66

incidents

- examples of, 59–60
- reporting, 61–62
- severity levels, 60

indicators of compromise (IoCs), 14, 480–481

infection routine, 18

inferential SQL injection, 33

information security (InfoSec), cybersecurity versus, 6–7

information sharing and coordination, 66

Information Technology Laboratory (ITL) bulletins, 7–8

infrastructure access controls, 179–182

Infrastructure as a Service (IaaS)

- customer versus provider security responsibility, 605–606
- definition of, 50–51, 582

infrastructure security, 344–345

control plane security

- CoPP (Control Plane Policing)*, 347, 397–399
- CPPr (Control Plane Protection)*, 348, 399
- process-switched traffic*, 395–397
- routing protocols*, 399–400
- routing update authentication on BGP*, 402–404
- routing update authentication on EIGRP*, 401
- routing update authentication on OSPF*, 400
- routing update authentication on RIP*, 401–402

IPv6 security

- ACLs (access control lists)*, 394–395
- best practices*, 388–389, 393–394
- focus on*, 390–391
- IPv4 versus*, 381–382
- IPv6 address format*, 383–384
- IPv6 address types*, 384–386
- moving to IPv6*, 388
- risks*, 391–392
- routing and routing protocols*, 386–388
- security plans*, 388
- threats*, 389–390

Layer 2 technology security

- importance of*, 320
- VLANs (virtual LANs) and trunking*, 320–331

Layer 2 threat mitigation. *See also* 802.1X; ACLs (access control lists)

- best practices*, 333–334
- BPDU Guard*, 334, 335–336
- CDP (Cisco Discovery Protocol)*, 338–339
- DAI (dynamic ARP inspection)*, 334, 341–343, 349, 390
- DHCP snooping*, 334, 339–341, 349
- dynamic ARP inspection*, 334, 341–343, 349
- LLDP (Link Layer Discovery Protocol)*, 338–339
- negotiations, preventing*, 334
- overview of*, 334–335
- port security*, 334, 336–338, 349
- Root Guard*, 334, 336
- logging, 360–361, 378–379
- management traffic security
 - AAA method lists*, 358, 364–369
 - best practices*, 354–356
 - Cisco IOS and Cisco NX-OS files*, 362
 - console cable*, 353–354
 - custom privilege levels*, 359, 371–373
 - definition of*, 350
 - encrypted management protocols*, 359–360
 - HTTPS (HTTP Secure)*, 359–360, 375–378
 - logging*, 360–361, 378–379
 - NETCONF (Network Configuration Protocol)*, 350–353
 - NTP (Network Time Protocol)*, 361, 379–380
 - parser views*, 359, 374–375
 - password recommendations*, 354, 356–357, 362–364
 - RBAC (role-based access control)*, 359
 - RESTCONF (RESTful Network Configuration Protocol)*, 350–353
 - router access authentication*, 357–358, 369–371
 - SNMP (Simple Network Management Protocol)*, 350–353
 - SSH (Secure Shell)*, 359–360, 375–378
 - user authentication*, 354, 357
- network infrastructure device image, 380–381
- NFP (Network Foundation Protection) framework
 - control plane security*, 344–345, 347–348, 395–404
 - data plane security*, 344–345, 348–349. *See also* IP (Internet Protocol)
 - implementation of*, 344–345
 - management plane security*, 344–347
 - overview of*, 343–344
- Initial Contact**, 501
- injection vulnerabilities
 - command injection, 33
 - examples of, 31
 - HTML injection, 33
 - SQL injection, 31–33, 53
- inline pair interfaces (Cisco Secure Firewall), 445
- inline pair with tap interfaces (Cisco Secure Firewall), 445–446
- Insecure Direct Object Reference vulnerabilities, 35–36
- INSTEON, 56
- Integrated Services Routers (ISRs), 238, 254, 419–421
- integrity, 45–46
- intent-based (northbound) APIs, 121, 135, 136

- interagency reports (NIST), 7
- inter-BVI communication, 444
- interface description languages (IDLs), 151
- interface modes, Cisco Secure Firewall, 442–444
 - inline pair, 445
 - inline pair with tap, 445–446
 - overview of, 442–444
 - passive mode, 446–447
 - passive with ERSPAN mode, 447
- interface types, Cisco Secure Web Appliance, 644
- interface Virtual-Access command, 511
- intermediate cache, NetFlow, 240
- Internal Endpoint Groups (IEPGs), 310
- International Data Encryption Algorithm (IDEA), 84
- International Organization for Standardization. *See* ISO (International Organization for Standardization)
- Internet Control Message Protocol (ICMP), 25–26, 349, 395, 462–463
- Internet edge, NetFlow deployment on, 258–259
- Internet Key Exchange. *See* IKE (Internet Key Exchange)
- Internet Message Access Protocol (IMAP), 477, 658
- Internet Protocol. *See* IP (Internet Protocol)
- Internet Protocol Flow Information Export. *See* IPFIX (Internet Protocol Flow Information Export)
- Internet Protocol Security. *See* IPsec (Internet Protocol Security) VPNs
- Internet Relay Chat (IRC), Trojan infection on, 21
- interpreter, Python, 138
- inter-VLAN routing, 326–327
- Intra-Site Automatic Tunnel Addressing Protocol (ISATAP), 281
- Introduction to Coding and APIs tutorial, 140
- intrusion detection systems (IDS), 420, 472
- intrusion prevention systems (IPSs), 349, 472
- Investigate, Cisco Umbrella, 610–611
- IoCs (indicators of compromise), 14, 480–481
- IOS/IOS-XE. *See* Cisco IOS/IOS-XE
- IoT (Internet of Things)
 - protocols, 56–57
 - security challenges and considerations, 54–57
 - tools and methods for hacking, 57
- IP (Internet Protocol)
 - accounting, 241
 - Anycast IP, 609
 - Block & Allow Lists, 681–682
 - covert communication, 25–26
 - geolocation, 613
 - IP Source Guard, 334, 349
 - IP-based access control policies, 131
 - IPv4
 - best practices*, 388–389
 - flow monitors*, 289–291
 - IPv6 versus*, 381–382
 - threats*, 389–390
 - IPv6 security, 25–26
 - ACLs (access control lists)*, 394–395
 - address format*, 383–384
 - address types*, 384–386
 - best practices*, 388–389, 393–394
 - flow monitors*, 289–291
 - focus on*, 390–391
 - IPv4 versus*, 381–382
 - IPv6 address format*, 383–384
 - IPv6 address types*, 384–386
 - moving to IPv6*, 388

- risks*, 391–392
 - routing and routing protocols*, 386–388
 - security plans*, 388
 - threats*, 389–390
 - spoofing, 653
 - ip flow monitor *name* input command, 293–294
 - ip ospf authentication-key command, 400
 - ip ospf message-digest-key command, 400
 - IP Security. *See* IPsec (Internet Protocol Security) VPNs
 - IPFIX (Internet Protocol Flow Information Export), 294
 - architecture, 251
 - mediators, 251–252
 - open-source tools, 250–251
 - option templates, 253–254
 - overview of, 249
 - SCTP (Stream Control Transmission Protocol), 254
 - templates, 252–253
 - ipfix keyword, 291
 - IPsec (Internet Protocol Security) VPNs, 93, 262, 494
 - in Cisco ASA, 538–540
 - IKE (Internet Key Exchange)
 - IKEv1 Phase 1 negotiation*, 496–498
 - IKEv1 Phase 2 negotiation*, 498–501
 - IKEv2*, 501–503
 - IPsec pass-through, 499
 - site-to-site VPNs in Cisco routers, 508–510
 - IPs (intrusion prevention systems), 349, 472
 - IRC (Internet Relay Chat), Trojan infection on, 21
 - Ironport. *See* Cisco Secure Email; Cisco Secure Web Appliance
 - IRPs (incident response plans), 62–63
 - ISA3000 firewall, 418–419
 - ISAKMP, 528–530
 - ISATAP (Intra-Site Automatic Tunnel Addressing Protocol), 281
 - ISE (Identity Services Engine). *See* Cisco ISE (Identity Services Engine)
 - ISO (International Organization for Standardization), 8. *See also* DFIR (digital forensics and incident response)
 - CSIRT (computer security incident response team) resources, 68–69
 - ISO/IEC 27000 series, 8
 - ISRs (Integrated Services Routers), 238, 254, 419–421
 - issuers, digital certificates, 99, 101
 - ITL (Information Technology Laboratory) bulletins, 7–8
-
- ## J
-
- JavaScript, 137
 - JIT (just-in-time) manufacturing, 586
 - JRE (Java Runtime Environment), 550–551
 - JSON (JavaScript Object Notation), 135
 - JWT (JSON Web Token), 173–174
-
- ## K
-
- Kadacoda website, 599
 - Kanban, 586
 - Katacoda, 595
 - KEM (key-encapsulation mechanism), 94
 - Kerberos, 174, 358, 654
 - key fields, Flexible NetFlow, 282–284
 - key incident management personnel, 75–76

keychain authentication, 404
 key-encapsulation mechanism (KEM), 94
 KeyGhost, 27
 keyloggers, 26–27
 keys, cryptographic, 83–84. *See also*
 PKI (public key infrastructure)
 GETVPN, 517
 key management, 92, 93
 key pairs, 85, 97
 pre-shared keys, 93, 497, 503
 keyspace, 92
 Kibana, 246
 Kind 19 option (TCP), 403
 knowledge, authentication by, 162–164
 krb5, 358
 krb5-telnet, 358
 kubctl version command, 598
 kubeadm, 599
 kubectrl get nodes command, 599, 601
 Kubernetes, 123, 419, 592, 597–602
 Kyber, 94

L

L2F (Layer 2 Forwarding), 494, 537
 L2TP (Layer 2 Tunneling Protocol), 494
 Lambda (AWS), 590
 Lancopé, 263
 languages, 137–140
 LANs (local area networks), 116–117
 Layer 2 broadcast domains. *See* VLANs
 (virtual LANs)
 Layer 2 Forwarding (L2F), 494, 537
 Layer 2 technologies, securing
 importance of, 320
 VLANs (virtual LANs)
 creation of, 321–323
 example of, 320–321
 inter-VLAN routing, 326–327

STP (Spanning Tree Protocol),
 328–332
 trunking, 323–326
 Layer 2 threats, mitigating. *See also*
 802.1X; ACLs (access control lists)
 best practices, 333–334
 BPDU Guard, 334, 335–336
 CDP (Cisco Discovery Protocol),
 338–339
 DAI (dynamic ARP inspection), 334,
 341–343, 349, 390
 DHCP snooping, 334, 339–341, 349
 dynamic ARP inspection, 334, 341–343,
 349
 LLDP (Link Layer Discovery Protocol),
 338–339
 negotiations, preventing, 334
 overview of, 334–335
 port security, 334, 336–338, 349
 Root Guard, 334, 336
 Layer 2 Tunneling Protocol (L2TP), 494
 LDAP (Lightweight Directory Access
 Protocol), 101, 653
 leaf-and-spine topology, 114
 Lean management philosophy, 585
 Learn Python.org, 137
 least privilege, principle of, 48, 161
 liability, cloud computing, 52, 608
 libraries, NBAR2 (Next Generation
 Network-Based Application
 Recognition), 132
 licenses, flow, 264
 Lightweight Access Point Protocol
 (LWAPP), 257
 Lightweight Directory Access Protocol
 (LDAP), 101, 653
 line password, 358
 Link Layer Discovery Protocol (LLDP),
 338–339
 link-local addresses, 384
 Linux commands

- cat, 86
 - curl, 141–143
 - dig, 658
 - md5sum, 87
 - shasum, 87
 - verify md5, 86
 - listeners, Cisco Secure Email, 660
 - lists, AAA method lists, 358, 364–369
 - LLDP (Link Layer Discovery Protocol), 338–339
 - local keyword, 358
 - local username database, 358
 - logging, 360–361
 - management plane best practices, 355
 - NEL (NetFlow Event Logging), 258
 - NSEL (NetFlow Secure Event Logging), 261
 - syslog, 245–246
 - configuration*, 378–379
 - severity levels*, 360–361
 - logical tunnel interfaces, 510–511
 - Login Password Retry Lockout feature, 354
 - Logstash, 246
 - Long Range Wide Area Network (LoRaWAN), 56
 - Low Power Wireless Personal Area Networks (6LoWPAN), 56
 - Low Rate Wireless Personal Area Networks (LRWPAN), 56
 - low-bandwidth attack, 60
 - LWAPP (Lightweight Access Point Protocol), 257
- M**
-
- MAB (MAC Authentication Bypass), 196, 213, 302, 305
 - MAC addresses, 336–338
 - machine learning, 40–41
 - macro infection, 16
 - MACs (mandatory access controls), 49, 177
 - mail. *See* email
 - mail delivery agents (MDAs), 658
 - mail exchanger (MX), 658–659
 - mail flow policies, 662
 - Mail Flow Summary dashboard, Cisco Secure Email, 663
 - mail submission agents (MSAs), 658
 - mail transfer agents (MTAs), 658
 - mail user agents (MUAs), 658
 - malware
 - analysis of
 - dynamic*, 29–30
 - static*, 28
 - covert communication, 24–26
 - distribution of, 22–23
 - keyloggers, 26–27
 - Malware Analytics Cloud
 - application control*, 683
 - Cisco Secure Endpoint*, 678
 - historical view of malware activity*, 677
 - IP blacklists and whitelists*, 680–681
 - payloads, 17–18
 - ransomware, 23–24
 - spyware, 16, 27–28
 - Trojans
 - communication methods*, 19
 - definition of*, 18
 - effects of*, 22
 - goals of*, 20–21
 - infection mechanisms*, 21–22
 - ports*, 19
 - types of*, 18–19
 - viruses
 - characteristics of*, 16

- malware payloads*, 17–18
- polymorphic*, 16–17
- transmission methods*, 16–17
- types of*, 16–17
- worms, 16
- Malware Analytics**, 479–483
- Malware Analytics Cloud**
 - application control, 683
 - Cisco Secure Endpoint, 678
 - historical view of malware activity, 677
 - IP blacklists and whitelists, 680–681
 - overview of, 675
- Malware Defense**
 - overview of, 478–483
 - Security Intelligence blocklisting, 483–484
 - Security Intelligence updates, 484
- Malware Threats report**, Cisco Secure Web Appliance, 656
- Management Access feature**, site-to-site VPNs, 536
- management and network orchestration (MANO)**, 123
- management plane**, 113. *See also* management traffic security
 - best practices, 344–347
 - overview of, 344–345
- management traffic security**, 362
 - AAA method lists, 358, 364–369
 - best practices, 354–356
 - Cisco IOS and Cisco NX-OS files, 362
 - console cable, 353–354
 - custom privilege levels, 359, 371–373
 - definition of, 350
 - encrypted management protocols, 359–360
 - HTTPS (HTTP Secure), 359–360, 375–378
 - logging, 360–361, 378–379
 - NETCONF (Network Configuration Protocol), 350–353
 - NTP (Network Time Protocol), 361, 379–380
 - benefits of*, 361
 - configuration*, 379–380
 - overview of*, 361
 - parser views, 359, 374–375
 - password recommendations, 354, 356–357, 362–364
 - RBAC (role-based access control), 359
 - RESTCONF (RESTful Network Configuration Protocol), 350–353
 - router access authentication, 357–358, 369–371
 - SNMP (Simple Network Management Protocol), 350–353
 - SSH (Secure Shell), 359–360, 375–378
 - user authentication, 354, 357
- management-access command**, 533–534
- mandatory access controls (MACs)**, 49, 177
- “Manifesto for Agile Software Development, The” 584
- man-in-the-browser attacks**, 35
- man-in-the-middle attacks**, 35, 390
- MANO (management and network orchestration)**, 123
- master boot record infection**, 16
- masters**, Kubernetes, 597
- Maximum Detection policy**, 474
- maximum transmission unit (MTU)**, 393, 536
- McAfee**, 643
- MD5 (Message Digest 5)**, 87–88, 93, 497
 - on BGP, 402–404
 - on EIGRP, 401
 - on OSPF, 400
 - on RIP, 401–402
- md5sum Linux command**, 87

- MDA (Multi-Domain Authentication), 214
- MDAs (mail delivery agents), 658
- mediators, IPFIX (Internet Protocol Flow Information Export), 251–252
- membership inference attacks, 41
- memory cards, 164
- Meraki, 176, 268, 691–692
- Mesos, 592
- Message Digest 5. *See* MD5 (Message Digest 5)
- message-digest keyword, 400
- messages
 - RADIUS, 182–184
 - TACACS+184
- metering process (MP), 251
- metrics
 - Cisco AVC (Application Visibility and Control), 255
 - CVSS (Common Vulnerability Scoring System), 69–73
- MFA (multifactor authentication), 34, 165, 357
- MGF (Multi Gigabit Fabric), 419
- micro-segmentation, 602–603
 - with Cisco ACI, 301
 - SDN (software-defined networking), 118–120
- Microsoft Account, 172
- Microsoft Active Directory, 101
- Microsoft Azure, 417
- Microsoft GPOs (Group Policy Objects), 645
- Microsoft SCVMM (System Center Virtual Machine Manager), 301
- Migration Tool, Cisco Secure Firewall, 415–416
- misconfiguration vulnerabilities, 9
- MITRE ATT&CK, 10, 21, 43, 271
- ML (machine learning), 40–41
- MMTF (multimode transparent firewall), 441
- MnT (Monitoring and Troubleshooting) node, 304
- mobile apps, Trojan infection on, 22
- Mobile IPv4 Application, 186
- mod_proxy module, 504
- Modbus, 419
- model inversion attack, 41
- model stealing attacks, 41
- models, cloud computing, 50–51
- Modular Policy Framework (MPF), 458
- monitor mode, 802.1X/TrustSec, 306
- monitoring
 - best practices, 355
 - cloud computing, 619–622
- Monitoring and Troubleshooting (MnT) node, 304
- MP (metering process), 251
- MPF (Modular Policy Framework), 458
- MPLS (Multiprotocol Label Switching), 262, 494, 515, 570
- MQTT, 57
- MSAs (mail submission agents), 658
- MTAs (mail transfer agents), 658
- MTU (maximum transmission unit), 393, 536
- MUAs (mail user agents), 658
- Multi Gigabit Fabric (MGF), 419
- multicast addresses, 385
- Multicast Rekeying, 516
- Multi-Domain Authentication (MDA), 214
- multifactor authentication (MFA), 34, 165, 357
- multilayer authentication, 165, 357
- multimode transparent firewall (MMTF), 441
- multipartite, 17

Multiple Authentication (Multi-Auth) modes, 214
 multipoint GRE (mGRE) tunnels, 512
 Multiprotocol Label Switching (MPLS), 262, 494, 515, 570
 multi-SA dVTI, 512
 multitенancy, 174
 multivendor support, Cisco DNA, 136
 Mutiny Fuzzing Framework, 604
 MX (mail exchanger), 658–659

N

nameif command, 437, 457
 NAS (Network Access Server), 205
 NAS-Filter-Rule, 205
 NAT (Network Address Translation)
 in Cisco ASA, 414, 458, 463–469
 NAT exempt policy, 534–535, 540
 NAT-T (NAT traversal), 499, 501, 536
 nat command, 534–535
 National Institute of Standards and Technology. *See* NIST (National Institute of Standards and Technology)
 National Vulnerability Database (NVD), 31, 43
 native VLANs (virtual LANs) on trunks, 326
 NAT-T (NAT traversal), 499, 501, 536
 NAT-Transparency-aware DMVPN, 514
 natural disasters, 12
 NBAR2 (Next Generation Network-Based Application Recognition), 132, 254–255, 280–281
 NBMA (Non-Broadcast Multiple Access), 512
 NDP (Network Discovery Protocol), 391
 need to know, 48, 161, 177
 negatives, false/true, 60
 neighbor cache resource starvation, 391
 NEL (NetFlow Event Logging), 258
 Nessus, 42
 NETCONF (Network Configuration Protocol), 147–148, 350–353
 NetFlow, 618
 anomaly detection, 241–243
 AVC (Application Visibility and Control), 254–255
 benefits of, 237–238
 cache, 240
 collection considerations and best practices, 279–280
 configuration in Cisco IOS and Cisco IOS-XE, 280–294
 configuration, 286–293
 flow exporters, 286, 291–293
 flow monitors, 286, 289–291, 293–294
 flow records, 287–289
 flow samplers, 286
 IPFIX export format, 294
 key fields, 282–284
 non-key fields, 284–285
 predefined records, 285
 records, 282
 simultaneous application tracking, 281–282
 user-defined records, 286
 configuration in NX-OS, 295–296
 data leak detection and prevention, 243
 DDoS attack mitigation, 241–243
 deployment, 239, 255–262
 data center, 259–261
 Internet edge, 258–259
 site-to-site and remote VPNs, 261–262
 user access layer, 256
 wireless LAN, 256–257
 five-tuple, 238–239
 flow, 238–241, 279–280

- incident response, 243–248
- IP Accounting versus, 241
- NEL (NetFlow Event Logging), 258
- network security forensics, 243–248
- NSEL (NetFlow Secure Event Logging), 261
- PDUs (protocol data units), 239
- scalability, 279–280
- security and visibility with, 241
- threat hunting with, 243–248
- traffic engineering and network planning, 248–249
- versions of, 249
- netflow-v5 keyword, 291**
- Netmaster, Contiv, 124**
- Netplugin, Contiv, 124**
- Network Access Server Application, 186**
- Network Access Server (NAS), 205**
- network ACLs (access control lists), 190–191**
- Network Address Translation. *See* NAT (Network Address Translation)**
- network analytics, 127, 263–264**
 - Cisco Cognitive Intelligence, 274–279
 - Cisco ETA (Encrypted Traffic Analytics), 274–279
 - dashboard, 268–270
 - FlowSensors, 238, 246, 260–261, 264
 - NetFlow. *See* NetFlow
 - network segmentation
 - application-based, 299–301*
 - with Cisco ISE, 302–312*
 - data-driven, 297–299*
 - micro-segmentation with Cisco ACI, 301*
 - types of, 296–297*
 - threat hunting with, 270–273
- Network Configuration Protocol (NETCONF), 147–148, 350–353**
- network device APIs (application programming interfaces), 145**
- Network Discovery Protocol (NDP), 391**
- Network Foundation Protection. *See* NFP (Network Foundation Protection) framework**
- Network Function Virtualization. *See* NFV (Network Function Virtualization)**
- network infrastructure. *See* infrastructure security**
- network overlays, 116–117**
- network programmability**
 - APIs (application programming interfaces), 140–141
 - documentation, 141*
 - gNMI (gRPC Network Management Interface), 151*
 - NETCONF, 147–148*
 - network device APIs, 145*
 - northbound, 121, 136*
 - OpenConfig, 151*
 - queryable, 141*
 - REST APIs, 135, 141–144*
 - RESTCONF, 149–151*
 - southbound, 121, 136*
 - technologies behind, 140–141*
 - YANG models, 145–146*
 - DevNet, 140
 - importance of, 136–137
 - programming languages and tools, 137–140
- Network Programmability Basics Video Course, 140**
- Network Programmability for Network Engineers tutorial, 140**
- network security solutions, comparison of, 435–436**
- network segmentation**
 - application-based, 299–301
 - with Cisco ISE, 302–312

- 802.1X/TrustSec in monitor mode*, 306
 - active policy enforcement*, 306–310
 - Cisco ACI integration*, 310–312
 - SGT assignment and deployment*, 306
 - SXP (SGT Exchange Protocol)*, 303–305
- data-driven, 297–299
- micro-segmentation with Cisco ACI, 301
- types of, 296–297
- Network Time Protocol. *See* NTP (Network Time Protocol)**
- network virtualization**
 - GENEVE (Generic Network Virtualization Encapsulation), 116
 - NFV (Network Function Virtualization)
 - architecture*, 121–123
 - NFV MANO*, 123
 - OPNFV (Open Platform for Network Function Virtualization)*, 122
 - NVGRE (Network Virtualization using Generic Routing Encapsulation), 116
 - VXLAN (Virtual Extensible LAN), 116
 - network overlays and*, 116–117
 - VTEP (VXLAN tunnel endpoint)*, 114
- Network Virtualization using Generic Routing Encapsulation (NVGRE)**, 116
- network visibility. *See also* network segmentation**
 - AVC (Application Visibility and Control), 254–255
 - Cisco Cognitive Intelligence, 274–279
 - Cisco ETA (Encrypted Traffic Analytics), 274
 - Cisco Secure Cloud Analytics, 242, 263–268
 - Cisco Secure Network Analytics, 263–264
 - dashboard*, 268–270
 - threat hunting with*, 270–273
- IPFIX (Internet Protocol Flow Information Export)
 - architecture*, 251
 - mediators*, 251–252
 - open-source tools*, 250–251
 - option templates*, 253–254
 - overview of*, 249
 - SCTP (Stream Control Transmission Protocol)*, 254
 - templates*, 252–253
- NetFlow. *See* NetFlow
 - overview of, 236
- Network Visibility Module (NVM)**, 262
- Network Watcher**, 265
- Network-Based Application Recognition (NBAR)**, 280–281
- Network-Based Application Recognition Version 2 (NBAR2)**, 254–255
- networking, software-defined. *See* SDN (software-defined networking)**
- networking planes**, 113
- networks**
 - as enforcers, 238
 - as sensors, 238
 - wireless, 133
- Neutron**, 120
- New Exclusion Set button, Cisco Secure Endpoint**, 684–686
- New IP List configuration**, 682
- Nexpose**, 42
- Next Generation Network-Based Application Recognition (NBAR2)**, 132
- Next Hop Resolution Protocol (NHRP)**, 512, 513
- next-generation encryption (NGE)**, 92–93
- next-generation firewalls (NGFW)**, 435

- Next-Generation IPS (NGIPS), 421–423, 476–478
- Nexus 1000V, 260–261
- NFP (Network Foundation Protection) framework, 343–344
 - control plane security
 - best practices*, 347–348
 - CoPP (Control Plane Policing)*, 347, 397–399
 - CPPr (Control Plane Protection)*, 348, 399
 - overview of*, 344–345, 395
 - process-switched traffic*, 395–397
 - routing protocols*, 399–400
 - routing update authentication on BGP*, 402–404
 - routing update authentication on EIGRP*, 401
 - routing update authentication on OSPF*, 400
 - routing update authentication on RIP*, 401–402
 - data plane security. *See also* IP (Internet Protocol)
 - best practices*, 348–349
 - overview of*, 344–345
 - implementation of, 344–345
 - management plane, 113, 344–347. *See also* management traffic security
 - best practices*, 344–347
 - overview of*, 344–345
- NFV (Network Function Virtualization)
 - architecture, 121–123
 - NFV MANO, 123
- NGE (next-generation encryption), 92–93
- NGFW (next-generation firewalls), 435
- NGIPSs (Next-Generation IPSs), 421–423, 476–478
- NHRP (Next Hop Resolution Protocol), 512, 513
- NIST (National Institute of Standards and Technology), 93–94
 - cybersecurity framework, 7
 - DFIR (digital forensics and incident response) guidelines, 58–59
 - interagency reports, 7
 - NVD (National Vulnerability Database), 43
 - Special Publication 500–292, 51, 582
 - Special Publication 800–52 Revision 2, 95
 - Special Publication 800–61, 59
 - Special Publication 800–61 Revision 2, 62–65, 244
 - Special Publication 800–63B, 163
 - Special Publication 800–145, 50
- No Rules Active policy, 474
- no shutdown command, 386
- no sysopt connection permit-vpn command, 534
- nodes, Kubernetes, 597
- no-execute (NX), 41
- Nomad, 592
- Non-Broadcast Multiple Access (NBMA), 512
- nondesignated ports, 331
- non-key fields, Flexible NetFlow, 284–285
- nonpublic personal information (NPPI), 44
- normal cache, NetFlow, 240
- northbound APIs (application programming interfaces), 121, 135, 136
- North-South traffic, 118, 259
- NPPI (nonpublic personal information), 44
- NSEL (NetFlow Secure Event Logging), 261
- NTLMSSP, 654
- Ntopng, 251

NTP (Network Time Protocol), 47, 100
 benefits of, 361
 best practices, 346, 355
 configuration, 379–380
 for IPv4/IPv6, 389
 overview of, 361

NULL bytes, 42

NVD (National Vulnerability Database), 31, 43

NVGRE (Network Virtualization using Generic Routing Encapsulation), 116

NVM (Network Visibility Module), 262

NX (no-execute), 41

O

OAS (OpenAPI Specification), 40, 141

OAuth, 174

object capability, 177

object grouping, Cisco ASA, 460–461

OCI (Open Container Initiative), 593

OCSP (Online Certificate Status Protocol), 95, 104, 655

ODL (OpenDaylight), 120–121

Offensive Security, Exploit Database, 10

Office 365, Cisco Secure Email Threat Defense, 615–616

offline brute-force attacks, 34

Ohno, Taiichi, 586

OllyDbg, 28

one-time pad (OTP), 84

one-time password (OTP), 84, 164

The Onion Router, 115

online brute-force attacks, 34

Online Certificate Status Protocol (OCSP), 95, 104, 655

on-path cryptographic attacks, 53

on-premises WAF (Web Application Firewall), 419

OOB (out-of-band), 346, 355

Open Authentication, 214

Open Command and Control (OpenC2), 15

Open Container Initiative (OCI), 593

Open DevSecOps GitHub organization, 603

Open Indicators of Compromise (OpenIOC), 15

Open Platform for Network Function Virtualization (OPNFV), 120–121, 122

open shortest path first (OSPF), 248, 347, 400, 414, 535

Open Virtual Network (OVN), 120–121

Open vSwitch Database Management Protocol (OVSDB), 121

Open vSwitch (OVS), 114, 120

Open Web Application Security Project (OWASP), 42

OpenAPI Specification (OAS), 40, 141

OpenC2 (Open Command and Control), 15

OpenConfig, 151

OpenDaylight (ODL), 120–121

OpenDNS, 609

OpenFlow, 114

OpenID, 172, 174

OpenIOC (Open Indicators of Compromise), 15

open-source initiatives
 Contiv, 123–124
 IPFIX (Internet Protocol Flow Information Export), 250–251
 SDN (software-defined networking), 120–121
 vulnerabilities, 42–43

OpenStack Neutron, 120

OPNFV (Open Platform for Network Function Virtualization), 120–121, 122

option templates, IPFIX, 253–254

OPTIONS method, 139
 Oracle Cloud, 417
 Organizationally Unique Identifier (OUI), 29
 organized crime groups, 13
 OSPF (open shortest path first), 248, 347, 400, 414, 535
 OTP (one-time password), 84, 164
 OUI (Organizationally Unique Identifier), 28
 Outbreak Control, Cisco Secure Endpoint
 application control, 683–684
 custom detections, 677–681
 IP blacklists and whitelists, 681–682
 out-of-band management, 164, 346, 355
 out-of-band SQL injection, 33
 outsourcing, 75
 overlays, 116–117
 OVN (Open Virtual Network), 120–121
 OVS (Open vSwitch), 114, 120
 OVSDB (OVS Database), 114, 121
 OWASP (Open Web Application Security Project), 42, 603
 ownership, authentication by, 164

P

Palo Alto Networks, 415–416
 PAN (Primary Administration Node), 223, 304
 parser views, 359, 374–375
 Parsing JSON using Python tutorial, 140
 passive DNA database, Cisco Umbrella, 612
 passive mode (Cisco Secure Firewall), 446–447
 passive with ERSPAN mode (Cisco Secure Firewall), 447
 PassiveID, 302, 305
 pass-through, IPsec, 499
 passwordless authentication, 175
 passwords
 cracking, 34–35
 guidelines for, 354, 356–357, 362–364
 Login Password Retry Lockout feature, 354
 OTP (one-time password), 84, 164
 PAT (Port Address Translation), 463–469
 patch management, 607–608
 Path exclusion type, 684
 pattern change evasion, 60
 payloads, malware, 17–18
 payment card information (PCI), 44
 PBR (policy-based routing), 646, 651–652
 PCI (payment card information), 44
 PCIe (Peripheral Component Interconnect Express), 419
 PDUs (protocol data units), 239
 Peach, 605
 Pearson Test Prep software, 697
 peer-to-peer networks (P2P), Trojan infection on, 21
 PeP (policy enforcement point), 189
 Perfect Forward Secrecy (PFS), 533, 535
 periodic parameter, time-based ACLs (access control lists), 462

- Peripheral Component Interconnect Express (PCIe), 419
- permanent cache, NetFlow, 240
- persistent cookies, Cisco Secure Web Appliance, 654
- persistent XSS attacks, 37
- personal identification number (PIN), 162
- personally identifiable information (PII), 12–13, 44
- personas, 304
- Per-VLAN Spanning Tree Plus (PVST+), 331
- PFS (Perfect Forward Secrecy), 533, 535
- PGP (Pretty Good Privacy), 97
- physical tunnel endpoint (PTEP), 114
- PII (personally identifiable information), 12–13, 44
- PIN (personal identification number), 162
- ping command, 25
- pip package (Python), 137
- pip3 install requests command, 144
- p-ipaddress ip_address command, 567
- pipelines, CI/CD, 588–589
- PKCS (Public Key Cryptography Standard), 86, 103
- PKI (public key infrastructure), 99–100, 497
 - asymmetric key cryptography, 97
 - CAs (certificate authorities), 98
 - authenticating and enrolling with*, 91, 102–103
 - cross-certifying*, 106
 - digital certificate enrollment with*, 91
 - hierarchical*, 105–106
 - single root*, 105
 - subordinate*, 105–106
 - definition of, 97
 - digital certificates
 - identity certificate*, 101
 - in practice*, 104–105
 - revoking*, 103–104
 - root certificates*, 99–100
 - digital signatures, 90–91, 97–98, 503
 - PGP (Pretty Good Privacy), 97
 - public and private key pairs, 85, 97
 - public key cryptography, 97
 - standards, 103
 - topologies, 105–106
 - X.500, 101–102
 - X.509v3, 101–102
- plaintext authentication, 401
- planes, networking, 113
- plans
 - DR/BCP (disaster recovery/business continuity plan), 52, 608
 - incident response, 62–63
- Platform as a Service (PaaS)
 - customer versus provider security responsibility, 605–606
 - definition of, 50–51, 582
- Platform Exchange Grid. *See* pxGrid (Platform Exchange Grid)
- platform settings policy, Cisco Secure Firewall, 476
- playbooks, incident response, 65–66
- POC (proof-of-concept) exploits, 10
- Pods, Kubernetes, 597
- Point-to-Point Tunneling Protocol (PPTP), 494, 537
- poison apple attacks, 20
- policies
 - active policy enforcement, 306–310
 - Cisco DNA (Digital Network Architecture)
 - application*, 131–132
 - Cisco DNA Center Policy Overview dashboard*, 127–129
 - group-based access control*, 129
 - IP-based access control*, 131

- traffic copy*, 132–133
- Cisco Firepower
 - Cisco NGIPS preprocessors*, 476–478
 - platform settings policy*, 476
 - variables*, 475–476
- Cisco ISE (Identity Services Engine), 199–201, 306–310
- Cisco Secure Email Threat Defense, 615, 661–662
- Cisco Secure Endpoint, 687–688
- Cisco Secure Firewall, 469–472
- Cisco Secure Web Appliance, 653–655
- client-based remote-access VPNs, 552–553
- clientless remote-access VPNs
 - group policies*, 544–545
 - policy inheritance model*, 544
- FlexConfig, 648
- IPsec remote-access VPNs in Cisco ASA, 539
- mail flow, 662
- PBR (policy-based routing), 651–652
- site-to-site VPNs
 - IPsec policy*, 531–532
 - NAT exempt policy*, 534–535
- SOCKS, 645–646
- policy enforcement point (PeP), 189
- Policy Service Nodes (PSNs), 223, 304
- policy-based routing (PBR), 646, 651–652
- policy-map command, 459
- polyalphabetic ciphers, 83
- polymorphic viruses, 17
- POP (Post Office Protocol), 477, 658
- Port Address Translation (PAT), 463–469
- ports
 - filtering, 399
 - security, 334, 336–338, 349
- SPAN (Switch Port Analyzer), 256
- STP (Spanning Tree Protocol) port states, 331
- TAPs (Test Access Ports), 256
- TCP (Transmission Control Protocol)
 - port 443*, 452, 503, 677
 - port 830*, 148
 - port 32137*, 677
- Trojans, 19
- UDP (User Datagram Protocol)
 - port 123*, 361, 380
 - port 500*, 498, 536
 - port 3799*, 206
 - port 4500*, 499, 536
- positives, false/true, 60
- possession, authentication by, 164
- POST method, 139
- Post Office Protocol (POP), 477, 658
- Post Quantum project website, 95
- Postman, 145
- post-quantum cryptography, 93–95
- posture assessment, Cisco ISE (Identity Services Engine), 203–204
- PPTP (Point-to-Point Tunneling Protocol), 494, 537
- Preboot Execution Environments (PXE), 214
- predefined records, Flexible NetFlow, 285
- predictive IP space monitoring model, 610
- preparation for SCOR 350–701 exam
 - final review and study, 696–697
 - hand-on preparation activities, 696
- prependers, 17
- preprocessors, NGIPSs, 421–423, 476–478
- pre-shared keys (PSK), 93, 497, 503
- pre-shared-key command, 531
- Pretty Good Privacy (PGP), 97

Primary Administration Node (PAN), 223, 304
 principle of least privilege, 48, 161
 private cloud, 582
 private key pairs, 85, 97
 privilege levels, custom, 359, 371–373
 Proactive Controls, OWASP, 603
 process-switched traffic, 395–397
 product security incident response teams (PSIRTs), 69
 profiles
 Cisco ISE (Identity Services Engine), 127, 195–198
 Cisco Secure Client, 566
 programmability, network. *See* network programmability
 programming languages, 137–140
 proof-of-concept (POC) exploits, 10
 protocol data units (PDUs), 239
 providers, Cisco Secure Workload, 624
 proxies
 Cisco Secure Web Appliance, 643–644, 653
 cloud-based, 610
 HTTPS proxy, 655
 reverse, 504
 proxy auto-configuration (PAC) files, 645
 proxy Trojans, 19
 PR-SCTP (Stream Control Transmission Protocol), 254
 PSIRTs (product security incident response teams), 69
 PSK (pre-shared key) authentication, 93, 497, 503
 PSNs (Policy Service Nodes), 223, 304
 PTEP (physical tunnel endpoint), 114
 public cloud, 582
 public key cryptography, 97
 Public Key Cryptography Standards (PKCS), 86, 103

public key infrastructure. *See* PKI (public key infrastructure)
 push protocols, 250
 PUT method, 139
 PVST+ (Per-VLAN Spanning Tree Plus), 331
 PXEs (Preboot Execution Environments), 214
 pxGrid (Platform Exchange Grid), 191
 Python, 137–140, 149–151
 Python Tutorial, 137

Q

QoS (quality of service), 131, 249
 Qualys, 42
 QuantumFlow Processor, 258
 queryable APIs, 141
 queue thresholding, 399

R

RaaS (Ransomware as a Service), 24
 race conditions, 39
 radio frequency identification (RFID), 257
 RADIUS, 357–358
 clientless remote-access VPNs in Cisco ASA, 547–548
 configuration, 213–215
 message exchange, 182–184
 TACACS+ versus, 185–186
 ransomware, 23–24
 Ransomware as a Service (RaaS), 24
 Rapid Spanning Tree, 332
 Rar, 23
 RAT (recipient access table), 661
 RATs (remote-access Trojans), 19
 RBAC (role-based access control), 49, 135, 178, 345–346, 354–355, 359

- recipient access table (RAT), 661
- Recorded Future, 43
- records, Flexible NetFlow, 282, 285–286, 287–289
- reflected XSS attacks, 36–37
- registries, container, 592
- regulatory requirements, cloud computing, 51
- Remote Access VPN Policy Wizard, 557–566
- Remote Authentication Dial-In User Service (RADIUS), 182–184, 185–186
- remote procedure call (RPC), 147–148
- remote-access Trojans (RATs), 19
- remote-access VPNs (virtual private networks), 570
 - Cisco SD-WAN RA, 569–573
 - in Cisco Secure Firewall, 554–555
 - overview of*, 556–557
 - Remote Access VPN Policy Wizard*, 557–566
 - troubleshooting*, 566–567
- client-based
 - Cisco Secure Client*, 553–554
 - DTLS (Datagram Transport Layer Security)*, 555–556
 - overview of*, 551
 - split tunneling*, 554–555
 - tunnel and group policies*, 552–553
- clientless
 - application access*, 550–551
 - attributes and policy inheritance model*, 544
 - clientless SSL VPNs, enabling*, 548–549
 - design considerations*, 541–542
 - group policies*, 544–545
 - pre-SSL VPN configuration*, 542–544
 - SSL VPN modes*, 540–541
 - tunnel groups*, 545–546
 - user authentication*, 546–548
 - WebType ACLs*, 549–550
- examples of, 494–496
- IPsec, 538–540
- NetFlow deployment on, 261–262
- reports and reporting
 - Cisco Secure Endpoint, 690–691
 - Cisco Secure Web Appliance, 655–657
 - Cisco Umbrella, 611
 - incidents, 61–62
- representational state transfer (REST), 40, 135, 141–144
- REQUEST, 187
- requests package (Python), 137
- Resource Reservation Protocol (RSVP), 395
- response, incident. *See* incident response
- REST (representational state transfer), 40, 135, 141–144
- RESTCONF, 149–151, 350–353
- return-to-libc, 41–42
- reverse proxy, 504
- reverse route injection (RRI), 535
- revoking digital certificates, 103–104
- RFCs (requests for comments)
 - RFC 2409, 496
 - RFC 2784, 508–509
 - RFC 2865, 182, 186
 - RFC 2866, 182, 186
 - RFC 2890, 508–509
 - RFC 3740, 510
 - RFC 4303, 500
 - RFC 5103, 249
 - RFC 5176.205
 - RFC 5996, 496, 501
 - RFC 6020, 145
 - RFC 6241, 147
 - RFC 6242, 147

RFC 6347, 555–556
 RFC 6407, 510, 516
 RFC 6526, 254
 RFC 7011, 249
 RFC 7015, 249
 RFC 7155, 187
 RFC 8040, 149
RFID (radio frequency identification), 257
RIP (Routing Information Protocol), 248, 401–402, 414
risk
 IPv6 security, 391–392
 RMF (risk management framework), 12–13
role-based access control (RBAC), 49, 135, 178, 345–346, 354–355, 359
root certificates, 99–100
Root Guard, 334, 336
root ports, 331
routed firewalls, 437–442
router access authentication, 357–358, 369–371
router-on-a-stick, 326–327
Routing Information Protocol (RIP), 248, 401–402, 414
routing protocol security, 399–400
routing update authentication
 on BGP, 402–404
 on EIGRP, 401
 on OSPF, 400
 on RIP, 401–402
RPC (Remote Procedure Call), 147–148
RRI (reverse route injection), 535
RSA algorithm, 86
rsa-signatures, 91
RSVP (Resource Reservation Protocol), 395
rule-based access control, 178

S

SaaS (Software as a Service), 174, 297
 customer versus provider security responsibility, 605–606
 definition of, 51, 582
 ThousandEyes, 124–125
same-security-traffic permit inter-interface command, 437
SAML (Security Assertion Markup Language), 166, 172–173, 175, 546–547
SAN (Secondary Administration Node), 223
sandboxing, 30, 478–483, 643, 675
SASE (secure access service edge), 570
SAST (static application security testing), 604–605
SCADA (supervisory control and data acquisition), 477
scalability, NetFlow, 279–280
SCEP (Simple Certificate Enrollment Protocol), 103
SCOR 350–701 exam
 exam updates, 698–700
 final review and study, 696–697
 hand-on preparation activities, 696
 Pearson Test Prep software, 697
script kiddies, 13
Scrum, 584–585
SCTP (Stream Control Transmission Protocol), 250, 254
SCVMM (Microsoft System Center Virtual Machine Manager), 301
SDLC (system development life cycle), 51, 72–73, 582, 603
SDN (software-defined networking)
 Cisco ACI (Application Centric Infrastructure)
 Cisco ACI Design Guide, 116

- Cisco ISE (Identity Services Engine) integration, 310–312*
- micro-segmentation, 301*
- overview of, 114–116*
- Cisco DNA (Digital Network Architecture). *See* Cisco DNA (Digital Network Architecture)
- controllers, 114
- micro-segmentation, 118–120
- network overlays, 116–117
- NFV (Network Function Virtualization)
 - architecture, 121–123*
 - NFV MANO, 123*
- open-source initiatives, 120–121, 123–124
- overview of, 112–113
- ThousandEyes integration, 124–125
- traditional networking compared to, 113
- VXLAN (Virtual Extensible LAN), 116–117
- SD-WANs (Software-Defined Wide Area Networks), 419–421, 569–573
- search routine, 18
- searchsploit, 11
- Secondary Administration Node (SAN), 223
- Secondary MNT (S-MNT), 223
- SecretCorp, 438
- secure access service edge (SASE), 570
- secure development life cycle (SDL), 72–73
- Secure Hash Algorithm. *See* SHA (Secure Hash Algorithm)
- secure issuance, 162
- Secure Shell, 355, 359–360, 375–378
 - for IPv4/IPv6, 389
 - port 22, 26
 - port 443, 26
 - preprocessor, 477
- Secure Sockets Layer. *See* SSL (Secure Sockets Layer)
- Secure/Multipurpose Internet Mail Extensions (S/MIME), 615
- SecureX, 426–429
- Security Assertion Markup Language (SAML), 166, 172–173, 175, 546–547
- security contexts, Cisco Secure Firewall, 438–439
- Security Dashboard, Cisco Secure Workload, 623–626
- security group ACL (SGACL), 192
- security group tags (SGTs), 192, 198, 201–203, 302
- security group-based ACLs (SGACLs), 191
- Security Information and Event Management (SIEM), 426–427, 627
- Security Intelligence
 - blocklisting, 483–484
 - updates, 484
- security labels, 177
- Security Management Appliance. *See* Cisco Content SMA (Security Management Appliance)
- security operations center (SOC), 632
- Security Orchestration, Automation, and Response (SOAR), 426–427, 627
- Security over Connectivity policy, 474
- security parameter index (SPI), 498
- Security solution, Cisco DNA, 135–136
- security zones, 431–432, 435
- security-software disablers, 19
- segmentation
 - application-based, 299–301
 - with Cisco ISE, 302–312
 - 802.1X/TrustSec in monitor mode, 306*
 - active policy enforcement, 306–310*
 - Cisco ACI integration, 310–312*

- SGT assignment and deployment*, 306
- SXP (SGT Exchange Protocol)*, 303–305
- data-driven, 297–299
- micro-segmentation, 118–120, 301, 602–603
- types of, 296–297
- SEI (Software Engineering Institute), 27, 73, 74–75
- Selective Packet Discard (SPD), 348
- semi-trusted networks, 297
- Sender Policy Framework (SPF), 615, 661–662
- SenderBase, 660–661
- sensors, networks as, 238
- separation of duties, 161
- serial numbers, digital certificates, 99, 101
- Serpent, 84
- serverless cloud computing, 589–591
- servers
 - 802.1X, 188–190
 - NETCONF (Network Configuration Protocol), 147–148
 - YANG (Yet Another Next Generation), 145–146
- server-side request forgery (SSRF), 38
- service level agreements (SLAs), 52, 608
- Service Lookup API, 195
- service-policy command, 459
- services, microservices, 602–603
- session cookies, Cisco Secure Web Appliance, 654
- session hijacking, 35, 53
- session riding attacks, 53
- session sniffing, 35
- session tokens, 35
- sessions, 240
- severity levels, 60, 361
- SGACLs (security group ACLs), 191, 192
- SGT Exchange Protocol (SXP), 303–305
- SGTs (security group tags), 192, 198, 201–203, 302, 303–305
- SHA (Secure Hash Algorithm), 93, 497
 - SHA-1, 88
 - SHA-2, 88
 - SHA-3, 88
 - SHA-256, 678–680
 - SHA-384, 89
 - SHA512 checksum, 86
- Shared Responsibility Model, 605
- shasum Linux command, 87
- Shodan, 35
- show access-list command, 460
- show command, 383
- show crypto ikev2 sa command, 524
- show crypto ikev2 sa detailed command, 524
- show crypto ikev2 session command, 524
- show crypto ikev2 stats command, 525
- show crypto isakmp sa command, 523–524
- show flow exporter command, 292
- show flow monitor command, 290
- show flow monitor name command, 292
- show flow record command, 289
- show interface trunk command, 324
- show interfaces Gi0/2 switchport command, 323
- show interfaces *interface* switchport command, 325
- show ip bgp neighbors | include Option Flags command, 403
- show ip cef command, 395–396
- show ipv6 route command, 388
- show monitor event-trace crypto ikev2 command, 527

- show monitor event-trace crypto ikev2 error all command, 528
- show monitor event-trace crypto ipsec command, 528
- show monitor event-trace crypto pki error all command, 528
- show monitor event-trace crypto pki event all command, 528
- show monitor event-trace crypto pki event internal all command, 528
- show monitor event-trace dmvpn command, 528
- show monitor event-trace gdoi command, 528
- show policy-map control-plane command, 397–399
- show run all sysopt command, 534
- show running-config flow exporter command, 292
- show running-config flow monitor command, 291
- show running-config flow record command, 289
- show vlan brief command, 322
- show vlan id command, 322
- side-channel attacks, 53
- SIEM (Security Information and Event Management), 426–427, 627
- SIG (secure Internet gateway), 610–611
- signatures
 - ClamAV, 680
 - digital, 90–91, 97–98
- Significant Compromise Artifacts list, 690
- Simple Certificate Enrollment Protocol (SCEP), 103
- Simple Mail Transfer Protocol (SMTP), 477, 661–662
- Simple Network Management Protocol (SNMP), 40, 242, 350–353, 360
- Simple Object Access Protocol (SOAP), 140–141
- simultaneous application tracking, Flexible NetFlow, 281–282
- single root CAs (certificate authorities), 105
- single sign-on (SSO), 171–173, 174–177, 653–654
- single-factor authentication, 357
- single-mode transparent firewall (SMTF), 439–441
- SIP preprocessor, 477
- site-to-site VPNs (virtual private networks)
 - in Cisco ASA, 537–538
 - advanced features*, 535–537
 - crypto maps*, 532–534
 - IPsec policy*, 531–532
 - ISAKMP, enabling*, 528–529
 - ISAKMP policy*, 529–530
 - NAT exempt policy*, 534–535
 - overview of*, 528–529
 - PFS (Perfect Forward Secrecy)*, 535
 - traffic filtering*, 534
 - tunnel groups*, 530–531
 - in Cisco routers
 - DMVPN*, 512–515
 - FlexVPN*, 518–522
 - GETVPN*, 512–518
 - GRE over IPsec*, 508–510
 - multipoint GRE (mGRE) tunnels*, 512
 - traditional site-to-site VPNs in Cisco IOS/Cisco IOS-XE*, 506–508
 - troubleshooting*, 522–528
 - tunnel interfaces*, 506–508, 510–512
 - in Cisco Secure Firewall, 567–569
 - examples of, 494–496
 - NetFlow deployment on, 261–262

- sizing Cisco ISE (Identity Services Engine) deployments, 224–225
- SKEYID, 498
- SLA (service level agreement), 52, 608
- Slack, 588
- Slot0, 419
- SMA (Security Management Appliance), 641–642, 662–667
- smart tunnels, 551
- smartcards, 164
- SMC (Stealthwatch Management Console), 276
- S/MIME (Secure/Multipurpose Internet Mail Extensions), 615
- S-MNT (Secondary MNT), 223
- SMS messages, Trojan infection on, 22
- SMSTF (single-mode transparent firewall), 439–441
- SMTP (Simple Mail Transfer Protocol), 477, 661–662
- sniffing, 390
- SNMP (Simple Network Management Protocol), 242, 350–353, 360
- snooping, DHCP, 334, 339–341, 349
- Snort, 422, 479, 484
- SOAP (Simple Object Access Protocol), 40, 140–141
- SOAR (Security Orchestration, Automation, and Response), 426–427, 627
- social identity providers (social IdPs), 175
- SOCKS proxy configurations, 645–646
- Softflowd, 250
- Software as a Service (SaaS), 174, 297
 - customer versus provider security responsibility, 605–606
 - definition of, 51, 582
- software development life cycle (SDLC), 586
- Software Engineering Institute (SEI), 27, 73, 74–75
- software vulnerabilities. *See* vulnerabilities
- software-defined networking. *See* SDN (software-defined networking)
- Software-Defined Wide Area Networks. *See* SD-WANs (Software-Defined Wide Area Networks)
- software/hardware vulnerabilities. *See* vulnerabilities
- solicited-node multicast addresses, 385
- SonarQube, 604
- Sophos, 643
- SOPs (standard operating procedures), 63
- SourceClear, 43
- SourceFire, 675
- southbound APIs (application programming interfaces), 121, 136
- SPAN (Switched Port Analyzer), 246, 256
- Spanning Tree Protocol (STP), 328–332, 390
- sparse infection, 17
- SPD (Selective Packet Discard), 348
- Spero, 480–481, 689
- SPF (Sender Policy Framework), 615
- SPI (security parameter index), 498
- split tunneling, 554–555
- Splunk, 246
- spoofing, 349, 390, 653
- Spring-MCV, 604
- sprints, 585
- spyware, 16, 27–28
- SQL injection, 31–33, 53
- SRUs (Snort rules updates), 484
- SSH (Secure Shell), 355, 359–360, 375–378
 - for IPv4/IPv6, 389
 - port 22, 26

- port 443, 26
- preprocessor, 477
- SSL (Secure Sockets Layer), 95–96, 104, 261, 494
 - clientless SSL VPNs, 548–549, 550–551
 - application access*, 550–551
 - enabling*, 548–549
 - preprocessors, 477
 - VPNs (virtual private networks), 503–504
- SSO (single sign-on), 171–173, 174–177, 653–654
- SSRF (server-side request forgery), 38
- SSVC (Stakeholder-Specific Vulnerability Categorization), 73
- Standalone mode, Cisco Secure Client, 553
- standard ACLs (access control lists), 455, 461
- standard keyword, 461
- standard operating procedures (SOPs), 63
- Stateless Transport Tunneling (STT), 116
- state-sponsored threat actors, 13
- static analysis, malware, 28
- static application security testing (SAST), 604–605
- static NAT (Network Address Translation), 463–469
- static VTI (sVTI), 512
- status codes, HTTP (Hypertext Transfer Protocol), 139
- Stealth AnyConnect, 204
- Stealthwatch. *See* Cisco Secure Network Analytics
- Stealthwatch Management Console (SMC), 276
- STIX (Structured Threat Information eXpression), 15, 481
- stored DOM-based attacks, 39
- stored XSS attacks, 37
- storm control, 335
- STP (Spanning Tree Protocol), 328–332, 390
- strcpy() function, 42
- stream ciphers, 84
- Stream Control Transmission Protocol (SCTP), 250, 254
- strong passwords, 354, 356–357, 362–364
- Structured Threat Information eXpression (STIX), 15, 481
- STT (Stateless Transport Tunneling), 116
- study plan
 - exam updates and, 698–700
 - final review and study, 696–697
 - hand-on preparation activities, 696
 - Pearson Test Prep software, 697
- Stuxnet, 28
- subjects, 161
- subordinate CAs (certificate authorities), 105–106
- substitution, 83
- Sun RPC preprocessor, 477
- supervisory control and data acquisition (SCADA), 477
- suplicants, 188
- surveillance spyware, 27
- sVTI (static VTI), 512
- Swagger (OpenAPI), 40, 141
- Swift, 137
- SWIM (Software Image Management), 135
- Switched Port Analyzer (SPAN), 246, 256
- SXP (SGT Exchange Protocol), 302, 303–305
- symmetric algorithms, 84–86
- Synopsys Protecode, 43
- syslog, 242, 245–246, 360–361, 378–379

sysopt connection permit-vpn command, 534

system development life cycle (SDLC), 51, 582, 603

T

- TACACS+357–358
- configuration, 207–212
 - message exchange, 184
 - RADIUS versus, 185–186
- TACXII (Trusted Automated eXchange of Indicator Information), 15
- Talos, 264, 422, 472–473, 479, 484, 610–611, 614, 643
- TAN (transaction authorization number), 19
- Tapestry, 604
- TAPs (Test Access Portss), 246, 256
- Tar, 23
- TAXII (Trusted Automated eXchange of Indicator Information), 481
- TCAM (Ternary Content-Addressable Memory), 511
- TCP (Transmission Control Protocol), 250
- covert communication, 25–26
 - port 443, 452, 503, 677
 - port 830, 148
 - port 32137, 677
 - TCP Intercept, 349
- TCSEC (Trusted Computer System Evaluation Criteria), 24
- TDN (trusted network detection), 262
- TE (traffic engineering), 248–249
- TEA (ThousandEyes Enterprise Agent), 124–125
- teams, CSIRTs (computer security incident response teams), 67–69, 74
- Telnet preprocessor, 476
- templates, 250, 252–253
- temporal agents, 203
- Teredo, 281
- Terminal Access Controller Access Control System Plus. *See* TACACS+
- terminal monitor command, 360
- Ternary Content-Addressable Memory (TCAM) tables, 511
- terrorist groups, 13
- test aaa command, 371
- Test Access Ports (TAPs), 246, 256
- TETRA, 689
- Tetration. *See* Cisco Secure Workload
- thin clients, 540
- ThousandEyes, 124–125
- threat actors, 13–14
- threat analytics, Cisco Secure Web Appliance, 643
- threat blocking, 676
- Threat Defense Virtual (Cisco Secure Firewall), 416–417
- threat detection preprocessors, 478
- Threat exclusion type, 684
- Threat Grid, 276, 612
- threat hunting, 243–248, 270–273
- threat intelligence, 14–16
- Threat Response. *See* incident response
- Threat Response dashboard (SecureX), 427–429
- Threat-Centric Network Access Control (TC-NAC), 204
- ThreatGRID, 478
- threats. *See also* malware
- access control management, 48–49
 - application layer attacks, 389–390
 - bot hosts/nets, 241, 414, 419
 - brute-force attack, 354
 - CAM table overflow attacks, 336
 - cloud computing, 50–54
 - attacks, 53
 - cloud computing models, 50–51

- issues and concerns*, 51–52
- security responsibilities*, 53–54
- DDoS (distributed denial-of-service) attacks, 13, 53, 241–243
- definition of, 8–9, 12–13
- dictionary attacks, 354
- DoS (denial-of-service) attacks, 13, 19, 46–48, 389–390, 502
- IoT (Internet of Things), 54–57
 - protocols*, 56–57
 - security challenges and considerations*, 54–56
 - tools and methods for hacking*, 57
- IPv4/IPv6, 389–390
- Layer 2 threat mitigation. *See also* 802.1X; ACLs (access control lists)
 - best practices*, 333–334
 - BPDU Guard*, 334, 335–336
 - CDP (Cisco Discovery Protocol)*, 338–339
 - DHCP snooping*, 334, 339–341, 349
 - dynamic ARP inspection*, 334, 341–343, 349
 - LLDP (Link Layer Discovery Protocol)*, 338–339
 - negotiations, preventing*, 334
 - overview of*, 334–335
 - port security*, 334, 336–338, 349
 - Root Guard*, 334, 336
- man-in-the-middle attacks, 390
- threat actors, 13–14
- threat intelligence, 14
- through-the-box traffic filtering, 456
- time of check to time of use (TOCTOU) attacks, 39
- time-based ACLs (access control lists), 461–462
- timestamps, syslog, 378–379
- Time-To-Live (TTL), 392, 396
- TLS (Transport Layer Security), 55, 95–96, 104, 503
- TOCTOU (time of check to time of use) attacks, 39
- Top-of-the-Rack (ToR) switches, 115
- topologies, PKI (public key infrastructure), 105–106
- ToS (type of service) byte, 239
- to-the-box traffic filtering, 459–460
- Toyota Production System, 585
- TRACE method, 139
- traffic copy policies, Cisco DNA, 132–133
- traffic engineering (TE), 248–249
- traffic redirection, WCCP configuration, 647–648
 - on Cisco Secure Web Appliance, 650–651
 - on Cisco switches, 649–650
- traffic spike model, 610
- transaction authorization number (TAN), 19
- transform sets, 506, 532
- transit sub-interface, 348
- transmission
 - Trojans, 20–21
 - viruses, 16–17
- Transmission Control Protocol. *See* TCP (Transmission Control Protocol)
- transparent firewalls, 437–442
- transparent mode, Cisco Secure Web Appliance, 646–647
- Transport Layer Security (TLS), 55, 95–96, 104, 503
- transport mode (IPsec), 500
- transport udp command, 291
- transposition, 83
- trigger routine, 18
- Triple Digital Encryption Standard (3DES), 84, 86, 93, 496

Trojans

- communication methods, 19
- definition of, 18
- effects of, 22
- goals of, 20–21
- infection mechanisms, 20–21
- ports, 19
- types of, 18–19

troubleshooting. *See also* debugging

- AAA (authentication, authorization, and accounting), 369–371
- remote-access VPNs in Cisco Secure Firewall, 566–567
- site-to-site VPNs in Cisco routers, 522–528
- TACACS+210–212

true positives/true negatives, 60**trunking, 323–326****Trusted Automated eXchange of Indicator Information (TAXII), 15, 481****Trusted Computer System Evaluation Criteria (TCSEC), 24****trusted network detection (TDN), 262****trusted networks, 296****TrustSec, 201–203, 306, 310–312****TTL (Time-to-Live), 392, 396****tunnel mode command, 511****tunnel mode gre multipoint command, 512****tunnel mode, IPsec, 500****tunnels, 116, 392**

- client-based remote-access VPNs, 552–553
- clientless remote-access VPNs, 545–546
- IPv6, 25–26
- site-to-site VPNs, 506–508, 510–512, 530–531
- STT (Stateless Transport Tunneling), 116

UDP (User Datagram Protocol), 26**tutorials**

- DevNet, 140
- Python, 137

Twofish, 84**type of service (ToS) byte, 239****U**

UCS (Unified Computing System), 419**UDP (User Datagram Protocol), 250, 291, 346**

- covert communication, 25–26
- port 123, 361, 380
- port 500, 498, 536
- port 3799, 206
- port 4500, 499, 536

Umbrella, 176

- architecture, 609–610
- Cisco Cognitive Intelligence integration, 276
- dashboard and reports, 611
- Investigate, 610–611
- overview of, 608–609
- SIG (secure Internet gateway), 610–611

undebug all command, 369**unicast addresses, 385****Unicast Reverse Path Forwarding (Unicast RPF), 396****Unified Computing System (UCS), 419****unprotected APIs (application programming interfaces), 39–40****untrusted networks, 297****updates**

- Cisco Secure Firewall, 484
- SCOR 350–701 exam, 698–700
- Security Intelligence, 484

uptime, 46**UPX, 28**

URL Categories report, Cisco Secure Web Appliance, 657

USB key drops, 20

US-CERT, 10

uSeg EPG, 301

user access layer, NetFlow deployment on, 256

User Datagram Protocol. *See* UDP (User Datagram Protocol)

user-defined records, Flexible NetFlow, 286

Users report, Cisco Secure Web Appliance, 655

V

VACLs (VLAN ACLs), 191

validity dates, digital certificates, 100

vAnalytics, 571–573

vCenter, 301

VDB (vulnerability database), 484

VDI (Virtual Desktop Infrastructure), 301

verify md5 Linux command, 86

VERIS community database, 162

VEX (Vulnerability Exploitability eXchange), 15

views, parser, 359, 374–375

Virtual Desktop Infrastructure (VDI), 301

Virtual Extensible LAN. *See* VXLAN (Virtual Extensible LAN)

virtual firewalls, 416–417

virtual LANs. *See* VLANs (virtual LANs)

virtual machine manager (VMM), 116

virtual machines (VMs), 193

virtual routing and forwarding (VRF), 116

virtualization, network. *See also* VPNs (virtual private networks)

GENEVE (Generic Network Virtualization Encapsulation), 116

NFV (Network Function Virtualization)

- architecture*, 121–123
- NFV MANO*, 123
- OPNFV (Open Platform for Network Function Virtualization)*, 122

NVGRE (Network Virtualization using Generic Routing Encapsulation), 116

STT (Stateless Transport Tunneling), 116

VDI (Virtual Desktop Infrastructure), 301

virtual firewalls, 416–417

VLANs (virtual LANs)

- creation of*, 321–323
- example of*, 320–321
- inter-VLAN routing*, 326–327
- STP (Spanning Tree Protocol)*, 328–332
- trunking*, 323–326

VMM (virtual machine manager), 116

VMs (virtual machines), 193

VRF (virtual routing and forwarding), 116

VTIs (Virtual Tunnel Interfaces), 511

VXLAN (Virtual Extensible LAN), 116

- network overlays and*, 116–117
- VNIDs (VXLAN Network Identifiers)*, 117
- VTEP (VXLAN tunnel endpoint)*, 114

Virtual-Tunnel Interface (VTI), 511

viruses

- characteristics of, 16
- malware payloads, 17–18
- polymorphic, 17
- transmission methods, 16–17
- types of, 16–17

visibility. *See* network visibility

- VLAN ACLs (VACLs), 191
- VLANs (virtual LANs)
 - creation of, 321–323
 - example of, 320–321
 - inter-VLAN routing, 326–327
 - STP (Spanning Tree Protocol), 328–332
 - trunking, 323–326
- vManage, 571–573
- VMM (virtual machine manager), 116
- VMs (virtual machines), 193
- VNIDs (VXLAN Network Identifiers), 117
- VoIP (voice over IP), 249
- VPC Flow Logs, 265
- VPNs (virtual private networks)
 - Cisco SD-WAN (Software-Defined Wide Area Network), 569–573
 - Cisco Secure Client Secure Mobility, 504–505
 - client-based remote-access
 - Cisco Secure Client*, 553–554
 - DTLS (Datagram Transport Layer Security)*, 555–556
 - overview of*, 551
 - split tunneling*, 554–555
 - tunnel and group policies*, 552–553
 - clientless remote-access
 - application access*, 550–551
 - attributes and policy inheritance model*, 544
 - clientless SSL VPNs, enabling*, 548–549
 - design considerations*, 541–542
 - group policies*, 544–545
 - pre-SSL VPN configuration*, 542–544
 - SSL VPN modes*, 540–541
 - tunnel groups*, 545–546
 - user authentication*, 546–548
 - WebType ACLs*, 549–550
 - clientless SSL
 - application access*, 550–551
 - enabling*, 548–549
 - FlexVPN, 511
 - IPsec (Internet Protocol Security), 538–540
 - IKE (Internet Key Exchange)*, 496–500, 501–503
 - IPsec pass-through*, 499
 - IPsec policy, 531–532
 - NAT-T (NAT traversal), 501
 - NetFlow deployment on, 261–262
 - protocols, 494
 - remote-access, 494–496
 - overview of*, 556–557
 - Remote Access VPN Policy Wizard*, 557–566
 - troubleshooting*, 566–567
 - site-to-site in Cisco ASA, 537–538
 - advanced features*, 535–537
 - crypto maps*, 531–532
 - examples of*, 494–496
 - ISAKMP, enabling*, 529
 - ISAKMP policy*, 529–530
 - NAT exempt policy*, 534–535
 - overview of*, 528–529
 - PFS (Perfect Forward Secrecy)*, 535
 - traffic filtering*, 534
 - tunnel groups*, 530–531
 - site-to-site in Cisco routers
 - DMVPN*, 512–515
 - FlexVPN*, 518–522
 - GETVPN*, 512–518
 - GRE over IPsec*, 508–510
 - multipoint GRE (mGRE) tunnels*, 512

- traditional site-to-site VPNs in Cisco IOS/Cisco IOS-XE, 506–508*
- troubleshooting, 522–528*
- tunnel interfaces, 506–508, 510–512*
- site-to-site in Cisco Secure Firewall, 567–569
- SSL (Secure Sockets Layer), 503–504
- VRF (virtual routing and forwarding), 116
- VSAs (vendor-specific attributes), 549
- VTEP (VXLAN tunnel endpoint), 114
- VTI (Virtual-Tunnel Interface), 511
- vtty lines, 360
- VulnDB, 43
- vulnerabilities. *See also* attacks; malware**
 - artificial intelligence and machine learning, 40–41
 - authentication-based, 33–36
 - buffer overflows, 41–42
 - cookie manipulation attacks, 39
 - CSRF (cross-site request forgery), 38
 - CVE (Common Vulnerabilities and Exposures), 10, 31
 - definition of, 9–10, 12–13
 - injection, 31–33
 - open-source software, 42–43
 - OWASP (Open Web Application Security Project), 42
 - race conditions, 39
 - return-to-libc, 41–42
 - SSRF (server-side request forgery), 38
 - unprotected APIs, 39–40
 - XSS (cross-site scripting), 33, 36–38, 53
- vulnerability database (VDB), 484**
- Vulnerability Exploitability eXchange (VEX), 15**
- VXLAN (Virtual Extensible LAN), 116**
 - network overlays and, 116–117
 - VNIDs (VXLAN Network Identifiers), 117
 - VTEP (VXLAN tunnel endpoint), 114

W

- W3 Schools Python tutorials, 137**
- WADL (Web Application Description Language), 40, 141**
- WAFs (Web Application Firewalls), 419**
- waterfall development methodology, 583**
- watering holes, 22**
- WCCP (Web Cache Communication Protocol), 646–651**
 - configuration in Cisco ASA, 647–648
 - configuration on Cisco Secure Web Appliance, 650–651
 - configuration on Cisco switches, 647–648
 - definition of, 646
 - transparent mode and, 646–647
- weather risk, 12**
- Web Application Description Language (WADL), 40, 141**
- Web Application Firewalls (WAFs), 419**
- Web Cache Communication Protocol. *See* WCCP (Web Cache Communication Protocol)**
- web filtering, 642**
- web identity, 175**
- web proxies, 653**
- Web Proxy Auto-Discovery (WPAD), 645**
- Web Reputation engine, 642**
- Web Services Description Language (WSDL), 40, 141**
- Web Sites report, 655**
- Web-enabled mode, Cisco Secure Client, 553**

Webex, 176
 Webroot, 643
 Webtype ACLs (access control lists),
 456, 549–550
 webvpn keyword, 544
 weighted random early detection
 (WRED), 255
 WEP (Wired Equivalent Privacy),
 34
 Whirlpool, 88, 93
 white hat hackers, 13–14
 whitelists, Cisco Secure Endpoint,
 681–682
 WhiteSource, 43
 Wi-Fi, 56
 Wildcard exclusion type, 684
 Windows identity, 175
 WinZip, 23
 Wired Equivalent Privacy (WEP), 34
 wired keyloggers, 27
 wireless keyloggers, 27
 wireless networks, 133
 WLANs (wireless LANs), NetFlow
 deployment on, 256–257
 WLCs (Wireless LAN Controllers),
 254
 Workload Optimization Manager,
 619–626
 worms, 16
 WPAD (Web Proxy Auto-Discovery),
 645
 wrappers, 23
 WRED (weighted random early
 detection), 255

WSDL (Web Services Description
 Language), 40, 141
 WS-Federation, 175

X

X.500, 101–102
 X.509v3, 101–102
 XACML (Extensible Access Control
 Markup Language), 179
 XDR (eXtended Detection and
 Response), 426–427, 618, 627–632
 XMPP (Extensible Messaging and
 Presence Protocol), 57, 193
 XSD (XML Schema Definition), 40,
 140–141
 XSRF (cross-site request forgery), 38
 XSS (cross-site scripting), 33, 36–38, 53

Y

YAF (Yet Another Flowmeter), 250
 YANG, 145, 351–353

Z

zero trust, 120, 169–171
 zero-day exploits, 10
 Zeus, 19
 Zigbee, 56
 zombies, 241
 Zone-Based Firewall (ZBFW), 182,
 435–436
 Z-Wave, 56