



**CCIE 8 Weeks**  
Learn. Practice. Achieve.



ALL-IN-ONE

# CCIE SECURITY V5.0

## WRITTEN EXAM 400-251 CERT GUIDE

Learn, Practice and Ace the New CCIE Written Exams with  
Test Prep Resources from CCIEin8Weeks™

CCIEin8Weeks.com

**PAUL ADAM, CCIE®**

3<sup>RD</sup> EDITION

## CCIE SECURITY V5.0 WRITTEN EXAM 400-251 CERT GUIDE

helped thousands of test takers and learners to  
s, practice and pass the CCIE® written exams  
Weeks™ contains supplemental resources such as  
study plans and blog articles to help you further  
ms and the real world. Our practice quizzes are  
to ensure your exam success.

side methodically and precisely covers all the  
CCIE® Security 400-251 V5.0 exam. It follows recently  
cial exam blueprint for CCIE® Security written  
er contains an Exam Essentials section at the end  
y concepts and to help you pass the exam.

- nce
- rimeter Security and Intrusion Prevention
- vanced Threat Protection and Content Security
- ure Connectivity and Segmentation
- ntity Management, Information Exchange, and
- ol
- rastructure Security, Virtualization, and Automation
- olving Technologies V1.1 – Cloud
- olving Technologies V1.1 – Network
- bility
- olving Technologies V1.1 – Internet of Things (IoT)

CCIEIN8WEEKS | FACEBOOK.COM/CCIEIN8WEEKS

CCIE 8 Weeks

CCIE 8 Weeks WRITTEN EXAM 400-251 V5.0 CERT GUIDE  
FOR CCIE® & CCNA PROFESSIONALS

3<sup>RD</sup> EDITION

SAM

**All-in-One CCIE Security V5.0  
400-251 Written Exam Cert Guide**

3rd Edition

SAMPLE GUIDE

FULL GUIDE HAS 500+ PAGES.

## Contents at a Glance

- Chapter 1 Perimeter Security and Intrusion Prevention
- Chapter 2 Advanced Threat Protection and Content Security
- Chapter 3 Secure Connectivity and Segmentation
- Chapter 4 Identity Management, Information Exchange, and Access Control
- Chapter 5 Infrastructure Security, Virtualization, and Automation
- Chapter 6 Evolving Technologies V1.1 - Cloud
- Chapter 7 Evolving Technologies V1.1 - Network Programmability
- Chapter 8 Evolving Technologies V1.1 - Internet of Things (IoTs)

SAMPLE GUIDE

## Table of Contents

<i>Preface</i> .....	26
<i>CCIE Security v5.0 Hardware and Software</i> .....	26
<i>Topics Added in CCIE Security v5.0 (versus V4.1)</i> .....	27
<i>Topics Removed in CCIE Security v5.0 (versus V4.1)</i> .....	27
<i>What this Exam Cert Guide Covers</i> .....	28
<i>How to Use this Exam Cert Guide</i> .....	28
<i>What's Available on the CCIEin8Weeks Website</i> .....	28
Chapter 1: Perimeter Security and Intrusion Prevention .....	30
<i>Chapter 1: Perimeter Security and Intrusion Prevention</i> .....	31
<i>Further Reading</i> .....	31
<i>Describe, implement, and troubleshoot HA features on Cisco ASA</i> .....	32
<i>Failover System Requirements</i> .....	32
<i>Hardware Requirements</i> .....	32
<i>Software Requirements</i> .....	32
<i>Licensing Requirements</i> .....	33
<i>Failover and Stateful Failover Links</i> .....	33
<i>Failover Link</i> .....	33
<i>Stateful Failover Link</i> .....	33
<i>Failover Interface Speed for Stateful Links</i> .....	34
<i>Avoiding Interrupted Failover Links</i> .....	35
<i>Active/Active and Active/Standby Failover</i> .....	35
<i>Determining Which Type of Failover to Use</i> .....	36
<i>Stateless (Regular) and Stateful Failover</i> .....	36
<i>Stateless Failover</i> .....	36
<i>Stateful Failover</i> .....	36
<i>Transparent Firewall Mode Requirements</i> .....	37
<i>Failover Health Monitoring</i> .....	38
<i>Unit Health Monitoring</i> .....	38
<i>Interface Monitoring</i> .....	38
<i>Further Reading</i> .....	39
<i>Describe, implement, and troubleshoot HA features on Cisco FirePOWER Threat Defense (FTD)</i> .....	39
<i>Hardware Requirements</i> .....	40
<i>High Availability System Requirements</i> .....	40
<i>Hardware Requirements</i> .....	40
<i>Software Requirements</i> .....	40
<i>License Requirements</i> .....	40
<i>Failover and Stateful Failover Links</i> .....	41

<i>Failover Link</i> .....	41
<i>Failover Link Data</i> .....	41
<i>Interface for the Failover Link</i> .....	41
<i>Connecting the Failover Link</i> .....	42
<i>Stateful Failover Link</i> .....	42
<i>Shared with the Failover Link</i> .....	42
<i>Dedicated Interface for the Stateful Failover Link</i> .....	42
<i>Avoiding Interrupted Failover and Data Links</i> .....	43
<i>Stateful Failover</i> .....	43
<i>Supported Features</i> .....	43
<i>Unsupported Features</i> .....	45
<i>Transparent Firewall Mode Bridge Group Requirements for Failover</i> .....	45
<i>Failover Health Monitoring</i> .....	45
<i>Unit Health Monitoring</i> .....	45
<i>Interface Monitoring</i> .....	46
<i>Failover Triggers and Detection Timing</i> .....	46
<i>Active/Standby Failover</i> .....	46
<i>Primary/Secondary Roles and Active/Standby Status</i> .....	46
<i>Configure Firepower Threat Defense High Availability</i> .....	47
<i>Further Reading</i> .....	48
<i>Describe, implement, and troubleshoot clustering on Cisco ASA</i> .....	48
<i>Licensing Requirements for ASA Clustering</i> .....	48
<i>ASA Hardware and Software Requirements</i> .....	49
<i>Master and Slave Unit Roles</i> .....	49
<i>Master Unit Election</i> .....	49
<i>Cluster Control Link Traffic Overview</i> .....	50
<i>Cluster Control Link Failure</i> .....	50
<i>Data Path Connection State Replication</i> .....	50
<i>ASA Clustering Configuration Procedure</i> .....	51
<i>Further Reading</i> .....	51
<i>Describe, implement, and troubleshoot clustering on Cisco FTD</i> .....	51
<i>Cluster Members</i> .....	52
<i>Primary and Secondary Unit Roles</i> .....	52
<i>Primary Unit Election</i> .....	52
<i>Cluster Interfaces</i> .....	52
<i>Cluster Control Link</i> .....	52
<i>Unsupported Features with Clustering</i> .....	53
<i>Centralized Features for Clustering</i> .....	53
<i>Add a Cluster to the Management Center</i> .....	53
<i>Further Reading</i> .....	54
<i><a href="https://goo.gl/Rn1UGY">https://goo.gl/Rn1UGY</a></i> .....	54
<i>Describe, implement, troubleshoot, and secure routing protocols on Cisco ASA</i> .....	54

<i>Egress Interface Selection Process</i> .....	55
<i>Next Hop Selection Process</i> .....	55
<i>Supported Internet Protocols for Routing</i> .....	56
<i>Displaying the Routing Table</i> .....	56
<i>Dynamic Routing and Failover</i> .....	57
<i>Dynamic Routing and Clustering</i> .....	57
<i>Dynamic Routing in Multiple Context Mode</i> .....	58
<i>Further Reading</i> .....	58
<i>Describe, implement, troubleshoot, and secure routing protocols on Cisco FTD</i> .....	59
<i>Determining the Egress Interface</i> .....	59
<i>Next Hop Selection Process</i> .....	59
<i>Supported Internet Protocols for Routing</i> .....	59
<i>Dynamic Routing and High Availability</i> .....	60
<i>Dynamic Routing in Clustering</i> .....	60
<i>Further Reading</i> .....	60
<i>Describe, implement, and troubleshoot different deployment modes such as routed, transparent, single, and multi-context on Cisco ASA</i> .....	61
<i>Routed Firewall Mode</i> .....	61
<i>Transparent Firewall Mode</i> .....	61
<i>Transparent Firewall Network</i> .....	61
<i>Allowing Layer 3 Traffic</i> .....	61
<i>Passing Traffic Not Allowed in Routed Mode</i> .....	61
<i>Common Use Cases for Security Contexts</i> .....	63
<i>Context Configurations</i> .....	63
<i>System Configuration</i> .....	64
<i>Admin Context Configuration</i> .....	64
<i>Enabling Multiple Context Mode</i> .....	64
<i>Further Reading</i> .....	64
<i>Describe, implement, and troubleshoot different deployment modes such as routed, transparent, single, and multi-context on Cisco FTD</i> .....	65
<i>Passing Traffic For Routed-Mode Features</i> .....	65
<i>Further Reading</i> .....	66
<i>Describe, implement, and troubleshoot firewall features such as NAT (v4,v6), PAT, application inspection, traffic zones, policy-based routing, traffic redirection to service modules, and identity firewall on Cisco ASA and Cisco FTD</i> .....	66
<i>Identity Policy Overview</i> .....	66
<i>Establishing User Identity through Active Authentication</i> .....	66
<i>Supported Directory Servers</i> .....	66
<i>Application Filtering</i> .....	67
<i>URL Filtering</i> .....	68
<i>Reputation-Based URL Filtering</i> .....	68
<i>Filtering HTTPS Traffic</i> .....	68

<i>Controlling Traffic by Encryption Protocol</i> .....	69
<i>Intrusion, File, and Malware Inspection</i> .....	69
<i>NAT and Access Rules</i> .....	69
<i>NAT Types</i> .....	70
<i>NAT Rule Order</i> .....	70
<i>Configure NAT</i> .....	71
<i>Pv6 NAT Guidelines</i> .....	71
<i>IPv6 NAT Recommendations</i> .....	71
<i>NAT Support for Inspected Protocols</i> .....	72
<i>Dynamic PAT</i> .....	72
<i>Install the SFR Module on the ASA</i> .....	73
<i>Further Reading</i> .....	73
<i>Describe, implement, and troubleshoot IOS security features such as Zone-Based Firewall (ZBF), application layer inspection, NAT (v4,v6), PAT and TCP intercept on Cisco IOS/IOS-XE</i> .....	74
<i>Zones and Inspection</i> .....	75
<i>Zones and ACLs</i> .....	75
<i>Access Control Lists and Class Maps</i> .....	75
<i>Supported Protocols for Layer 3 and Layer 4</i> .....	75
<i>Firewall and Network Address Translation</i> .....	76
<i>Out-of-Order Packet Processing Support in the Zone-Based Firewalls</i> .....	76
<i>Smart Licensing Support for Zone-Based Policy Firewall</i> .....	77
<i>Configuring a Class Map for a Layer 3 and Layer 4 Firewall Policy</i> .....	77
<i>Creating a Policy Map for a Layer 3 and Layer 4 Firewall Policy</i> .....	78
<i>Creating Security Zones and Zone Pairs and Attaching a Policy Map to a Zone Pair</i> .....	78
<i>Configuring Static Translation of Inside Source Addresses</i> .....	79
<i>Configuring Dynamic Translation of Inside Source Addresses</i> .....	80
<i>Using NAT to Allow Internal Users Access to the Internet (PAT)</i> .....	80
<i>Using Application-Level Gateways with NAT</i> .....	81
<i>NAT Support of H.323 v2 RAS</i> .....	81
<i>NAT Support for H.323 v3 and v4 in v2 Compatibility Mode</i> .....	81
<i>NAT H.245 Tunneling Support</i> .....	81
<i>NAT Support of Skinny Client Control Protocol</i> .....	82
<i>NAT Support of SCCP Fragmentation</i> .....	82
<i>NAT Segmentation with Layer 4 Forwarding</i> .....	82
<i>Further Reading</i> .....	84
<i>Describe, implement, optimize, and troubleshoot policies and rules for traffic control on Cisco ASA, Cisco FirePOWER and Cisco FTD</i> .....	84
<i>License Requirements for Access Control</i> .....	84
<i>Creating a Basic Access Control Policy</i> .....	85
<i>Blacklisting Using Security Intelligence IP Address Reputation</i> .....	85
<i>Tuning Traffic Flow Using Access Control Rules</i> .....	86
<i>Controlling Traffic with Network-Based Rules</i> .....	87



<i>Controlling Traffic Based on Users</i> .....	88
<i>Controlling Traffic Using Intrusion and File Policies</i> .....	88
<i>Understanding Network Analysis and Intrusion Policies</i> .....	89
<i>Further Reading</i> .....	90
<i>Describe, implement, and troubleshoot Cisco Firepower Management Center (FMC) features such as alerting, logging, and reporting</i> .....	90
<i>Firepower Management Center Capabilities</i> .....	91
<i>Report Templates</i> .....	91
<i>Firepower Management Center Alert Responses</i> .....	92
<i>Configurations Supporting Alert Responses</i> .....	92
<i>Configuring Impact Flag Alerting</i> .....	93
<i>Configuring Discovery Event Alerting</i> .....	93
<i>Configuring AMP for Firepower Alerting</i> .....	94
<i>Configuring Discovery Event Alerting</i> .....	94
<i>Configuring AMP for Firepower Alerting</i> .....	95
<i>External Alerting for Intrusion Events</i> .....	95
<i>Further Reading</i> .....	95
<i>Describe, implement, and troubleshoot correlation and remediation rules on Cisco FMC</i> .....	96
<i>The Remediation Subsystem</i> .....	97
<i>Using the Remediation Subsystem</i> .....	98
<i>Correlation Policies and Rules</i> .....	98
<i>Correlation Rules</i> .....	98
<i>Compliance White Lists</i> .....	99
<i>Correlation Responses</i> .....	99
<i>Correlation and Multi Tenancy</i> .....	99
<i>Configuring Correlation Policies</i> .....	99
<i>Further Reading</i> .....	100
<i>Describe, implement, and troubleshoot Cisco FirePOWER and Cisco FTD deployment such as in-line, passive, and TAP modes</i> .....	100
<i>IPS Device Deployment and Configuration</i> .....	101
<i>Passive IPS Deployments</i> .....	101
<i>Passive Interfaces on the Firepower System</i> .....	101
<i>Inline IPS Deployments</i> .....	101
<i>Advanced Inline Set Options</i> .....	102
<i>Tap Mode</i> .....	102
<i>Propagate Link State</i> .....	102
<i>Transparent Inline Mode</i> .....	103
<i>Strict TCP Enforcement</i> .....	103
<i>Further Reading</i> .....	103
<i>Describe, implement, and troubleshoot Next Generation Firewall (NGFW) features such as SSL inspection, user identity, geolocation, and AVC (Firepower appliance)</i> .....	103
<i>Configurations</i> .....	104



Troubleshooting.....	104
Issue 1: Some websites may not load on the Chrome browser .....	104
Issue 2: Getting an untrusted warning/error in some browsers.....	104
Verify and Troubleshoot.....	108
Verify Connectivity between FMC and User Agent (Passive Authentication).....	109
Verify Connectivity between FMC and Active Directory .....	109
Verify Connectivity between Firepower Sensor and End system (Active Authentication).....	109
Verify Policy configuration & Policy Deployment .....	109
Analyse the Events logs.....	109
Geolocation Database Update.....	110
Further Reading .....	110
Describe, detect, and mitigate common types of attacks such as DoS/DDoS, evasion techniques, spoofing, man-in-the-middle, and botnet.....	110
Further Reading .....	112
Exam Essentials.....	113
Chapter 2: Advanced Threat Protection and Content Security.....	114
Chapter 2: Advanced Threat Protection and Content Security.....	115
Compare and contrast different AMP solutions including public and private cloud deployment models .....	115
Deployment Modes.....	115
Comparison of AMP Private and Public Cloud Deployments .....	116
Further Reading .....	118
Describe, implement, and troubleshoot AMP for networks, AMP for endpoints, and AMP for content security (CWS, ESA, and WSA) .....	118
Deployment Options for Protection Everywhere.....	118
AMP for networks.....	119
Further Reading .....	123
AMP for endpoints.....	123
Further Reading .....	129
AMP for content security (CWS, ESA, and WSA).....	129
Further Reading .....	130
Detect, analyze, and mitigate malware incidents .....	130
Further Reading .....	131
Describe the benefit of threat intelligence provided by AMP Threat GRID .....	131
Cisco AMP Threat Grid Overview.....	131
Further Reading .....	133
Perform packet capture and analysis using Wireshark, tcpdump, SPAN, and RSPAN .....	133
Capturing Packets.....	133
Filtering Packets.....	134
Inspecting Packets .....	137
Packet capture using SPAN and RSPAN.....	138

<i>Describe, implement, and troubleshoot web filtering, user identification, and Application Visibility and Control (AVC) .....</i>	<i>139</i>
<i>Further Reading .....</i>	<i>144</i>
<i>Describe, implement, and troubleshoot mail policies, DLP, email quarantines, and SenderBase on ESA .....</i>	<i>144</i>
<i>Mail Policies on ESA .....</i>	<i>144</i>
<i>DLP on ESA (SSN Example) .....</i>	<i>145</i>
<i>Create a Custom Policy .....</i>	<i>145</i>
<i>Create a Classifier .....</i>	<i>145</i>
<i>Set the Severity Settings .....</i>	<i>145</i>
<i>Set the Severity Scale .....</i>	<i>146</i>
<i>Submit and Commit Changes.....</i>	<i>146</i>
<i>Final Steps.....</i>	<i>147</i>
<i>Quarantine on ESA .....</i>	<i>147</i>
<i>SenderBase on ESA.....</i>	<i>147</i>
<i>Further Reading .....</i>	<i>148</i>
<i>Describe, implement, and troubleshoot SMTP authentication such as SPF and DKIM on ESA .....</i>	<i>148</i>
<i>Inbound SMTP Authentication.....</i>	<i>148</i>
<i>Outbound SMTP Authentication.....</i>	<i>148</i>
<i>Further Reading .....</i>	<i>149</i>
<i>Describe, implement, and troubleshoot SMTP encryption on ESA .....</i>	<i>149</i>
<i>Enable Email Encryption on the ESA .....</i>	<i>149</i>
<i>Create an Outgoing Content Filter.....</i>	<i>150</i>
<i>Verify.....</i>	<i>150</i>
<i>Validate Encryption Filter Processing in the Mail_logs .....</i>	<i>150</i>
<i>Further Reading .....</i>	<i>151</i>
<i>Describe, implement, and troubleshoot WCCP redirection .....</i>	<i>151</i>
<i>Redirect Traffic with WCCP (CLI).....</i>	<i>151</i>
<i>Further Reading .....</i>	<i>152</i>
<i>Compare and contrast different proxy methods such as SOCKS, Auto proxy/WPAD, and transparent.....</i>	<i>153</i>
<i>Further Reading .....</i>	<i>155</i>
<i>Describe, implement, and troubleshoot HTTPS decryption and DLP.....</i>	<i>155</i>
<i>Root Certificates.....</i>	<i>155</i>
<i>Server Certificates.....</i>	<i>156</i>
<i>DLP on WSA.....</i>	<i>156</i>
<i>Further Reading .....</i>	<i>157</i>
<i>Describe, implement, and troubleshoot CWS connectors on Cisco IOS routers, Cisco ASA, Cisco AnyConnect, and WSA .....</i>	<i>157</i>
<i>Further Reading .....</i>	<i>158</i>
<i>Cisco ASA Configuration for Redirection to CWS .....</i>	<i>160</i>
<i>Further Reading .....</i>	<i>161</i>
<i>WSA as a Connector to CWS.....</i>	<i>161</i>

<i>Native Connector as a Connector to CWS</i> .....	162
<i>Further Reading</i> .....	163
<i>Describe, implement, and troubleshoot SMA for centralized content security management</i> .....	163
<i>Describe the security benefits of leveraging Lancope</i> .....	166
<i>Further Reading</i> .....	167
<i>Exam Essentials</i> .....	167
Chapter 3: Secure Connectivity and Segmentation.....	169
<i>Chapter 3: Secure Connectivity and Segmentation</i> .....	170
<i>Compare and contrast cryptographic and hash algorithms such as AES, DES, 3DES, ECC, SHA, MD5, ISAKMP/IKEv1, IKEv2, SSL, TLS/DTLS, ESP, AH, SAP, and MKA</i> .....	170
<i>Asymmetric key algorithms (Public key cryptography)</i> .....	170
<i>Hashing functions</i> .....	171
<i>Further Reading</i> .....	172
MD5 .....	173
<i>Further Reading</i> .....	173
SHA.....	173
<i>Further Reading</i> .....	173
DES/3DES .....	173
<i>Further Reading</i> .....	174
AES .....	174
<i>Further Reading</i> .....	175
IPsec .....	175
<i>Further Reading</i> .....	177
ISAKMP.....	177
<i>Table, ISAKMP policy commands, keywords and their meaning</i> .....	177
<i>Further Reading</i> .....	180
IKE and IKEv2 .....	180
<i>Benefits of IKEv2</i> .....	180
<i>Further Reading</i> .....	181
<i>Describe, implement and troubleshoot remote access VPN using technologies such as FLEXVPN, SSL-VPN between Cisco firewalls, routers, and end hosts</i> .....	181
<i>Cisco IOS FlexVPN Features and Benefits</i> .....	181
<i>Configuring FlexVPN in a Site to Site VPN Setup</i> .....	182
PSK Tunnel Configuration .....	183
Left-Router .....	183
Right-Router.....	184
PKI Tunnel Configuration .....	184
Left-Router .....	184
Right-Router.....	186
Verify.....	186
Routing Configuration.....	187
Dynamic Routing Protocols.....	187

<i>Further Reading</i> .....	190
<i>SSL VPN Overview</i> .....	190
<i>Licensing</i> .....	191
<i>Licensing in Cisco IOS Release 15.x</i> .....	192
<i>Remote Access Overview</i> .....	192
<i>Clientless Mode</i> .....	192
<i>Thin-Client Mode</i> .....	193
<i>Tunnel Mode</i> .....	193
<i>Further Reading</i> .....	193
<i>Describe, implement, and troubleshoot the Cisco IOS CA for VPN authentication</i> .....	194
<i>Configuring the Cisco IOS CA Server</i> .....	194
<i>Further Reading</i> .....	200
<i>Describe, implement, and troubleshoot clientless SSL VPN technologies with DAP and smart tunnels on Cisco ASA and Cisco FTD</i> .....	200
<i>Configure Clientless SSL VPN (WebVPN) on the ASA using ASDM</i> .....	200
<i>Configuration Steps</i> .....	200
<i>Verify</i> .....	201
<i>Troubleshoot</i> .....	201
<i>Procedures Used to Troubleshoot</i> .....	201
<i>Further Reading</i> .....	202
<i>Cisco ASA Dynamic Access Policies (DAP)</i> .....	202
<i>Further Reading</i> .....	202
<i>Cisco ASA and Smart Tunnels</i> .....	202
<i>Further Reading</i> .....	203
<i>Describe, implement, and troubleshoot site-to-site VPNs such as GETVPN, DMVPN and IPsec</i> .....	203
<i>Cisco Group Encrypted Transport VPN Architecture</i> .....	204
<i>GDOI</i> .....	204
<i>Group Member</i> .....	204
<i>Key Server</i> .....	204
<i>How Protocol Messages Work with Cisco Software</i> .....	205
<i>Communication Flow Between Key Servers and Group Members to Update IPsec SAs</i> .....	205
<i>IPsec and ISAKMP Timers</i> .....	206
<i>Address Preservation</i> .....	207
<i>Secure Data Plane Multicast</i> .....	207
<i>Secure Data Plane Unicast</i> .....	207
<i>Configuring a Key Server</i> .....	207
<i>Configuring the Group ID Server Type and SA Type</i> .....	207
<i>Configuring the Rekey</i> .....	208
<i>Configuring Group Member ACLs</i> .....	208
<i>Configuring an IPsec Lifetime Timer</i> .....	209
<i>Configuring an ISAKMP Lifetime Timer</i> .....	209
<i>Configuring the IPsec SA</i> .....	209

<i>Configuring Time-Based Anti Replay for a GDOI Group</i> .....	210
<i>Configuring Passive SA</i> .....	210
<i>Configuring a Group Member</i> .....	210
<i>Configuring the Group Name ID Key Server IP Address and Group Member Registration</i> .....	210
<i>Creating a Crypto Map Entry</i> .....	211
<i>Activating Fail-Close Mode</i> .....	211
<i>Configuring GETVPN GM Authorization</i> .....	211
<i>Verifying and Troubleshooting Cisco Group Encrypted Transport VPN Configurations</i> .....	211
<i>Verifying States and Statistics for All Features and All Debug Levels</i> .....	212
<i>Further Reading</i> .....	212
<i>Benefits of Dynamic Multipoint VPN (DMVPN)</i> .....	212
<i>Hub Router Configuration Reduction</i> .....	212
<i>Automatic IPsec Encryption Initiation</i> .....	212
<i>Support for Dynamically Addressed Spoke Routers</i> .....	212
<i>Dynamic Creation for Spoke-to-Spoke Tunnels</i> .....	213
<i>VRF Integrated DMVPN</i> .....	213
<i>VRF Integrated DMVPN</i> .....	213
<i>NAT-Transparency Aware DMVPN</i> .....	214
<i>Call Admission Control with DMVPN</i> .....	214
<i>NHRP Rate-Limiting Mechanism</i> .....	214
<i>DMVPN Configuration Steps</i> .....	214
<i>Configuring an IPsec Profile</i> .....	214
<i>Configuring the Hub for DMVPN</i> .....	215
<i>Configuring the Spoke for DMVPN</i> .....	215
<i>Configuring the Forwarding of Clear-Text Data IP Packets into a VRF</i> .....	216
<i>Configuring the Forwarding of Encrypted Tunnel Packets into a VRF</i> .....	216
<i>Further Reading</i> .....	216
<i>Site to Site IPsec Tunnels (also known as LAN to LAN Tunnels)</i> .....	216
<i>Router A Configuration</i> .....	217
<i>Router B Configuration</i> .....	218
<i>Verify</i> .....	220
<i>Troubleshoot</i> .....	221
<i>Further Reading</i> .....	221
<i>Describe, implement, and troubleshoot uplink and downlink MACsec (802.1AE)</i> .....	222
<i>Downlink MACsec</i> .....	223
<i>Uplink MACsec</i> .....	223
<i>Configuration Examples for WAN MACsec and MKA Example:</i> .....	223
<i>Point-to-point, CE to CE Connectivity Using EPL Service</i> .....	223
<i>Further Reading</i> .....	227
<i>Describe the functions and security implications of cryptographic protocols such as SAP, MKA, SCEP/EST, GDOI, X.509, WPA, WPA2, WEP, and TKIP</i> .....	228
<i>Further Reading</i> .....	228

<i>Further Reading</i> .....	229
<i>WEP, WEP, WPA, and WPA2</i> .....	229
<i>Further Reading</i> .....	231
<i>SXP</i> .....	231
<i>Security Group Tagging</i> .....	231
<i>Using CTS-SXP for SGT Propagation Across Legacy Access Networks</i> .....	231
<i>Further Reading</i> .....	232
<i>MACSec</i> .....	232
<i>Further Reading</i> .....	233
<i>WPA, WEP and WPA2</i> .....	233
<i>Further Reading</i> .....	234
<i>SXP</i> .....	234
<i>Security Group Tagging</i> .....	235
<i>Using CTS-SXP for SGT Propagation Across Legacy Access Networks</i> .....	235
<i>Further Reading</i> .....	235
<i>MACSec</i> .....	235
<i>Further Reading</i> .....	236
<i>Describe the security benefits of network segmentation and isolation</i> .....	236
<i>Policy-Based Path Isolation</i> .....	237
<i>Further Reading</i> .....	238
<i>Describe, implement, and troubleshoot VRF-Lite and VRF-Aware VPN</i> .....	238
<i>FlexVPN Server Configuration</i> .....	238
<i>Verify</i> .....	241
<i>Derived Virtual Access Interface</i> .....	241
<i>Crypto Sessions</i> .....	242
<i>Further Reading</i> .....	243
<i>Describe, implement, and troubleshoot microsegmentation with TrustSec using SGT and SXP</i> .....	243
<i>Further Reading</i> .....	246
<i>Describe, implement, and troubleshoot infrastructure segmentation methods such as VLAN, PVLAN, and GRE</i> .....	246
<i>Deploying Path Isolation using VRF-Lite and MPLS VPN</i> .....	246
<i>Design Options—Three Deployment Models</i> .....	246
<i>Deploying Path Isolation Using VRF-Lite and GRE</i> .....	246
<i>Control Plane-Based Path Isolation</i> .....	246
<i>Further Reading</i> .....	247
<i>Describe the functionality of Cisco VSG used to secure virtual environments</i> .....	247
<i>Further Reading</i> .....	249
<i>Describe the security benefits of data center segmentation using ACI, EVPN, VXLAN, and NVGRE</i> .....	249
<i>Security benefits of Cisco ACI</i> .....	249
<i>Further Reading</i> .....	253
<i>Security benefits of VXLAN and BGP-based EVPN</i> .....	253
<i>MP-BGP EVPN Control Plane: Overview</i> .....	254

<i>Further Reading</i> .....	256
<i>Exam Essentials</i> .....	256
Chapter 4: Identity Management, Information Exchange, and Access Control .....	258
<i>Chapter 4: Identity Management, Information Exchange, and Access Control</i> .....	259
<i>Describe, implement, and troubleshoot various personas of ISE in a multinode deployment</i>	259
<i>Types of Nodes</i> .....	259
<i>Understanding Distributed Deployment</i> .....	260
<i>Setting Up a Distributed ISE Deployment</i> .....	262
<i>Configuring a Cisco ISE Node</i> .....	262
<i>Changing Node Personas and Services</i> .....	264
<i>Further Reading</i> .....	265
<i>Describe, implement, and troubleshoot network access device (NAD), ISE, and ACS configuration for AAA</i> .....	265
<i>Further Reading</i> .....	266
<i>Using TACACS+ with ACS</i> .....	267
<i>Using RADIUS with ACS</i> .....	267
<i>CS 5.8 as the AAA Server</i> .....	267
<i>Describe, implement, and troubleshoot AAA for administrative access to Cisco network devices using ISE and ACS</i> .....	268
<i>AAA for administrative access to Cisco network devices using ISE</i> .....	268
<i>Add Network Device</i> .....	269
<i>Enable Device Admin Service</i> .....	269
<i>Configuring TACACS Command Sets</i> .....	269
<i>Configuring TACACS Profile</i> .....	269
<i>Configuring TACACS Authorization Policy</i> .....	270
<i>Configure the Cisco IOS Router for Authentication and Authorization</i> .....	270
<i>Verify</i> .....	271
<i>Cisco IOS Router Verification</i> .....	271
<i>Further Reading</i> .....	272
<i>AAA for administrative access to Cisco network devices using ACS</i> .....	272
<i>Further Reading</i> .....	274
<i>Describe, implement, verify, and troubleshoot AAA for network access with 802.1X and MAB using ISE</i> .....	274
<i>Deploying Cisco Identity Services Engine</i> .....	275
<i>Configure MAC Authentication Bypass (MAB)</i> .....	276
<i>Configure 802.1X for wired and wireless users</i> .....	276
<i>Enabling Visibility to the Wired Network</i> .....	277
<i>Further Reading</i> .....	277
<i>Describe, implement, verify, and troubleshoot cut-through proxy/auth-proxy using ISE as the AAA server</i> .....	277
<i>SGA Features</i> .....	277
<i>Further Reading</i> .....	279



<i>Describe, implement, verify, and troubleshoot guest life cycle management using ISE and Cisco network infrastructure.....</i>	<i>279</i>
<i>ISE Guest lifecycle management.....</i>	<i>280</i>
<i>WLC Interaction for Local WebAuth .....</i>	<i>281</i>
<i>Wired NAD Interaction for Central WebAuth .....</i>	<i>281</i>
<i>Wired NAD Interaction with Local WebAuth .....</i>	<i>283</i>
<i>Further Reading .....</i>	<i>283</i>
<i>Describe, implement, verify, and troubleshoot BYOD on-boarding and network access flows with an internal or external CA.....</i>	<i>283</i>
<i>Identity Certificate for ISE.....</i>	<i>284</i>
<i>Network Device Definition within ISE .....</i>	<i>284</i>
<i>ISE Integration with Active Directory.....</i>	<i>285</i>
<i>Guest and Self-Registration Portals.....</i>	<i>285</i>
<i>ISE Using Certificates as an Identity Store .....</i>	<i>285</i>
<i>Identity Source Sequences .....</i>	<i>286</i>
<i>SCEP Profile Configuration on ISE .....</i>	<i>286</i>
<i>Authentication Policies .....</i>	<i>286</i>
<i>Authentication Policy for Wireless.....</i>	<i>287</i>
<i>Client Provisioning .....</i>	<i>288</i>
<i>Enabling the DHCP and RADIUS Probes.....</i>	<i>288</i>
<i>Logical Profiles .....</i>	<i>288</i>
<i>Certificate Authority Server .....</i>	<i>289</i>
<i>NDES Server Configuration for SCEP.....</i>	<i>289</i>
<i>Certificate Template .....</i>	<i>289</i>
<i>Further Reading .....</i>	<i>289</i>
<i>Describe, implement, verify, and troubleshoot ISE and ACS integration with external identity sources such as LDAP, AD, external RADIUS, RADIUS Token, RSA SecurID, and SAML.....</i>	<i>290</i>
<i>Certificate Authentication Profiles.....</i>	<i>290</i>
<i>Adding or Editing a Certificate Authentication Profile .....</i>	<i>291</i>
<i>Microsoft Active Directory.....</i>	<i>291</i>
<i>Key Features of the Integration of Cisco ISE and Active Directory .....</i>	<i>292</i>
<i>Supported Authentication Protocols.....</i>	<i>292</i>
<i>Further Reading .....</i>	<i>292</i>
<i>Cisco ISE and RSA SecurID Server Integration.....</i>	<i>292</i>
<i>RSA Configuration in Cisco ISE.....</i>	<i>292</i>
<i>RSA Agent Authentication Against the RSA SecurID Server.....</i>	<i>293</i>
<i>RSA Identity Sources in a Distributed Cisco ISE Environment .....</i>	<i>293</i>
<i>RSA Server Updates in a Cisco ISE Deployment .....</i>	<i>293</i>
<i>Add RSA Identity Sources .....</i>	<i>293</i>
<i>Import the RSA Configuration File .....</i>	<i>293</i>
<i>Cisco ISE and SAML Integration.....</i>	<i>294</i>
<i>Add a SAML Identity Provider .....</i>	<i>295</i>

<i>Further Reading</i> .....	298
<i>Describe, implement, verify, and troubleshoot provisioning of AnyConnect with ISE and ASA</i> .....	298
<i>Configuration Steps</i> .....	299
<i>Configure</i> .....	299
<i>WLC</i> .....	299
<i>ISE</i> .....	299
<i>Step 1. Add the WLC</i> .....	299
<i>Step 2. Configure the VPN Profile</i> .....	300
<i>Step 3. Configure the NAM Profile</i> .....	300
<i>Step 4. Install the Application</i> .....	300
<i>Step 5. Install the VPN/NAM Profile</i> .....	300
<i>Step 6. Configure the Posture</i> .....	300
<i>Step 7. Configure AnyConnect</i> .....	301
<i>Step 8. Client Provisioning Rules</i> .....	301
<i>Step 9. Authorization Profiles</i> .....	301
<i>Step 10. Authorization Rules</i> .....	302
<i>Verify</i> .....	302
<i>Further Reading</i> .....	302
<i>Describe, implement, verify, and troubleshoot posture assessment with ISE</i> .....	302
<i>Components of Posture Services</i> .....	302
<i>Posture Administration Services</i> .....	303
<i>Posture Runtime Services</i> .....	303
<i>Posture and Client-Provisioning Policies Workflow</i> .....	303
<i>Posture Service Licenses</i> .....	304
<i>Posture Service Deployment</i> .....	304
<i>Run the Posture Assessment Report</i> .....	305
<i>Further Reading</i> .....	305
<i>Describe, implement, verify, and troubleshoot endpoint profiling using ISE and Cisco network infrastructure including device sensor</i> .....	305
<i>Configure</i> .....	306
<i>Step 1. Standard AAA configuration</i> .....	306
<i>Step 2. Configure Device Sensor</i> .....	307
<i>Step 3. Configure profiling on ISE</i> .....	307
<i>Verify</i> .....	308
<i>Troubleshoot</i> .....	308
<i>Step 1. Verify information collected by CDP/LLDP</i> .....	308
<i>Step 2. Check Device Sensor cache</i> .....	308
<i>Step 3. Check if attributes are present in Radius Accounting</i> .....	308
<i>Further Reading</i> .....	308
<i>Describe, implement, verify, and troubleshoot integration of MDM with ISE</i> .....	308
<i>Default Network Device Definition in Cisco ISE</i> .....	309
<i>Create a Network Device Definition in Cisco ISE</i> .....	310

<i>Set Up MDM Servers With Cisco ISE</i> .....	310
<i>Import MDM Server Certificate into Cisco ISE</i> .....	311
<i>Further Reading</i> .....	312
<i>Describe, implement, verify, and troubleshoot authentication methods such as EAP Chaining and Machine Access Restriction (MAR)</i> .....	312
<i>MAR as a Solution</i> .....	313
<i>The Pros</i> .....	313
<i>The Cons</i> .....	313
<i>MAR and Microsoft Windows Supplcant</i> .....	313
<i>MAR and Various RADIUS Servers</i> .....	314
<i>MAR and Wired-wireless Switching</i> .....	314
<i>Further Reading</i> .....	315
<i>Describe the functions and security implications of AAA protocols such as RADIUS, TACACS+, LDAP/LDAPS, EAP (EAP-PEAP, EAP-TLS, EAP-TTLS, EAP-FAST, EAP-TEAP, EAP- MD5, EAP-GTC), PAP, CHAP, and MS-CHAPv2</i> .....	315
<i>Further Reading</i> .....	315
<i>Describe, implement, and troubleshoot identity mapping on ASA, ISE, WSA and FirePOWER</i> .....	315
<i>Further Reading</i> .....	315
<i>Describe, implement, and troubleshoot pxGrid between security devices such as WSA, ISE, and Cisco FMC</i> .....	315
<i>Cisco Identity Service Engine Dynamic Security Group Tags</i> .....	317
<i>Further Reading</i> .....	320
<i>Exam Essentials</i> .....	320
<b>Chapter 5: Infrastructure Security, Virtualization, and Automation</b> .....	321
<i>Chapter 5: Infrastructure Security, Virtualization, and Automation</i> .....	322
<i>Identify common attacks such as Smurf, VLAN hopping, and SYNful knock, and their mitigation techniques</i> .....	322
<i>Further Reading</i> .....	322
<i>SYNful Knock</i> .....	322
<i>Further Reading</i> .....	323
<i>Describe, implement, and troubleshoot device hardening techniques and control plane protection methods, such as CoPP and IP Source routing</i> .....	324
<i>CoPP</i> .....	324
<i>Further Reading</i> .....	325
<i>IP Source Routing</i> .....	326
<i>Further Reading</i> .....	326
<i>Describe, implement, and troubleshoot management plane protection techniques such as CPU and memory thresholding and securing device access</i> .....	326
<i>Memory Threshold Notifications</i> .....	326
<i>CPU Thresholding Notification</i> .....	327
<i>Secure Interactive Management Sessions</i> .....	328
<i>Authentication, Authorization, and Accounting</i> .....	328

<i>Further Reading</i> .....	328
<i>Describe, implement, and troubleshoot data plane protection techniques such as iACLs, uRPF, QoS, and RTBH</i> .....	329
<i>Unicast RP</i> .....	329
<i>RTBH</i> .....	330
<i>Further Reading</i> .....	332
<i>Describe, implement, and troubleshoot IPv4/v6 routing protocols security</i> .....	332
<i>Secure BGP</i> .....	332
<i>TTL-based Security Protections</i> .....	332
<i>BGP Peer Authentication with MD5</i> .....	333
<i>Configure Maximum Prefixes</i> .....	334
<i>Filter BGP Prefixes with Prefix Lists</i> .....	334
<i>Filter BGP Prefixes with Autonomous System Path Access Lists</i> .....	335
<i>Secure Interior Gateway Protocols</i> .....	336
<i>Routing Protocol Authentication and Verification with Message Digest 5</i> .....	336
<i>Passive-Interface Commands</i> .....	338
<i>Route Filtering</i> .....	338
<i>Routing Process Resource Consumption</i> .....	339
<i>Further Reading</i> .....	340
<i>Describe, implement, and troubleshoot Layer 2 security techniques such as DAI, IPDT, STP security, port security, DHCP snooping, and VACL</i> .....	340
<i>DAI</i> .....	340
<i>Further Reading</i> .....	341
<i>IPDT</i> .....	341
<i>Functionality Areas</i> .....	341
<i>Disable IPDT</i> .....	342
<i>Further Reading</i> .....	342
<i>STP Security</i> .....	342
<i>Further Reading</i> .....	344
<i>Port Security</i> .....	344
<i>Further Reading</i> .....	345
<i>DHCP Snooping</i> .....	345
<i>Trusted and Untrusted Sources</i> .....	345
<i>Further Reading</i> .....	346
<i>VACL</i> .....	346
<i>Further Reading</i> .....	346
<i>Describe, implement, and troubleshoot wireless security technologies such as WPA, WPA2, TKIP, and AES</i> .....	346
<i>Further Reading</i> .....	347
<i>Describe wireless security concepts such as FLEX Connect, wIPS, ANCHOR, Rogue AP, and Management Frame Protection (MFP)</i> .....	347
<i>FLEX Connect</i> .....	347

<i>FlexConnect Authentication Process</i> .....	347
<i>Further Reading</i> .....	347
<i>wIPS</i> .....	347
<i>Further Reading</i> .....	348
<i>ANCHOR</i> .....	348
<i>Further Reading</i> .....	349
<i>Rogue AP</i> .....	349
<i>Further Reading</i> .....	349
<i>Management Frame Protection (MFP)</i> .....	349
<i>Further Reading</i> .....	350
<i>Describe, implement, and troubleshoot monitoring protocols such as NETFLOW/IPFIX, SNMP, SYSLOG, RMON, NSEL, and eSTREAMER</i> .....	350
<i>NetFlow</i> .....	350
<i>Further Reading</i> .....	351
<i>SNMP</i> .....	351
<i>Table, the SNMP manager and MIB operations</i> .....	351
<i>Further Reading</i> .....	353
<i>Syslog</i> .....	353
<i>Further Reading</i> .....	354
<i>RMON</i> .....	354
<i>Further Reading</i> .....	355
<i>NSEL</i> .....	355
<i>Further Reading</i> .....	357
<i>eSTREAMER</i> .....	357
<i>Further Reading</i> .....	358
<i>Describe the functions and security implications of application protocols such as SSH, TELNET, TFTP, HTTP/HTTPS, SCP, SFTP/FTP, PGP, DNS/DNSSEC, NTP, and DHCP</i> .....	358
<i>SSH</i> .....	358
<i>TELNET</i> .....	359
<i>TFTP</i> .....	359
<i>HTTP/HTTPS</i> .....	360
<i>SCP</i> .....	360
<i>Further Reading</i> .....	361
<i>SFTP/FTP</i> .....	361
<i>Further Reading</i> .....	361
<i>PGP</i> .....	362
<i>Further Reading</i> .....	362
<i>DNS/DNSSEC</i> .....	362
<i>Difference between DNS and DNSSEC</i> .....	363
<i>Further Reading</i> .....	364
<i>NTP</i> .....	364
<i>DHCP</i> .....	364

<i>Further Reading</i> .....	365
<i>Describe the functions and security implications of network protocols such as VTP, 802.1Q, TCP/UDP, CDP, LACP/PAgP, BGP, EIGRP, OSPF/OSPFv3, RIP/RIPng, IGMP/CGMP, PIM, IPv6, and WCCP</i> .....	365
VTP .....	365
<i>Further Reading</i> .....	365
802.1Q.....	365
TCP/UDP.....	366
CDP.....	366
LACP/PAgP .....	367
BGP.....	367
<i>Further Reading</i> .....	367
EIGRP, OSPF/OSPFv3, RIP/RIPng.....	367
Routing Protocol Authentication and Verification with Message Digest 5 .....	367
Passive-Interface Commands.....	369
Route Filtering.....	370
Routing Process Resource Consumption.....	371
IGMP/CGMP.....	372
PIM.....	373
PIM Neighbor Control .....	373
<i>Further Reading</i> .....	374
IPv6 .....	374
<i>Further Reading</i> .....	377
WCCP.....	377
<i>Further Reading</i> .....	378
<i>Describe the benefits of virtualizing security functions in the data center using ASAv, WSAv, ESAv, and NGIPSv</i> .....	378
<i>Further Reading</i> .....	379
<i>Further Reading</i> .....	379
Reclaim the Visibility Lost When Virtualizing .....	380
Deploy Protection Easier and Wider.....	380
Extend Payment Card Industry (PCI) Compliance to Virtual Environments.....	381
<i>Further Reading</i> .....	382
<i>Describe the security principles of ACI such as object models, endpoint groups, policy enforcement, application network profiles, and contracts</i> .....	382
<i>Describe the northbound and southbound APIs of SDN controllers such as APIC-EM</i> .....	386
<i>Further Reading</i> .....	387
<i>Identify and implement security features to comply with organizational security policies, procedures, and standards such as BCP 38, ISO 27001, RFC 2827, and PCI-DSS</i> .....	387
BCP 38.....	387
<i>Further Reading</i> .....	388
ISO 27001.....	388
<i>Further Reading</i> .....	388

<i>RFC 2827</i> .....	388
<i>Further Reading</i> .....	389
<i>PCI-DSS</i> .....	389
<i>Further Reading</i> .....	391
<i>Describe and identify key threats to different places in the network (campus, data center, core, edge) as described in Cisco SAFE</i> .....	391
<i>Customer Use Cases</i> .....	392
<i>WAN Edge</i> .....	393
<i>Campus</i> .....	393
<i>Intranet Data Center</i> .....	394
<i>Further Reading</i> .....	394
<i>Validate network security design for adherence to Cisco SAFE recommended practices</i> .....	394
<i>Key Threats in the Infrastructure</i> .....	395
<i>Infrastructure Device Access</i> .....	395
<i>Routing Infrastructure</i> .....	396
<i>Device Resiliency and Survivability</i> .....	397
<i>Network Telemetry</i> .....	397
<i>Network Policy Enforcement</i> .....	398
<i>Switching Infrastructure</i> .....	398
<i>Design Principles</i> .....	398
<i>Defense-in-Depth</i> .....	398
<i>Service Availability and Resiliency</i> .....	399
<i>Regulatory Compliance</i> .....	399
<i>Modularity and Flexibility</i> .....	399
<i>Strive for Operational Efficiency</i> .....	399
<i>Further Reading</i> .....	399
<i>Interpret basic scripts that can retrieve and send data using RESTful API calls in scripting languages such as Python</i> .....	400
<i>SA REST API Requests and Responses</i> .....	400
<i>Request Structure</i> .....	400
<i>Response Structure</i> .....	400
<i>Install and Configure the ASA REST API Agent and Client</i> .....	402
<i>JavaScript</i> .....	402
<i>Python</i> .....	402
<i>Perl</i> .....	402
<i>Enabling REST API Debugging on the ASA</i> .....	403
<i>Further Reading</i> .....	403
<i>Describe Cisco Digital Network Architecture (DNA) principles and components</i> .....	403
<i>Further Reading</i> .....	405
<i>Exam Essentials</i> .....	405
Chapter 6: Compare and Contrast Public, Private, Hybrid, and Multi-cloud Design Considerations .....	407
<i>Public Cloud</i> .....	408



<i>Private Cloud</i> .....	409
<i>Virtual Private Cloud (VPC)</i> .....	409
<i>Hybrid Cloud</i> .....	410
<i>Multi-cloud</i> .....	411
<i>Infrastructure as a service (IaaS)</i> .....	412
<i>Platform as a service (PaaS)</i> .....	413
<i>Software as a Service (SaaS)</i> .....	413
<i>Consolidation</i> .....	415
<i>Virtualization</i> .....	415
<i>Automation</i> .....	415
<i>Performance, Scalability, and High Availability</i> .....	415
<i>Performance</i> .....	415
<i>Scalability and High Availability</i> .....	417
<i>Security Implications, Compliance, and Policy</i> .....	418
<i>Workload Migration</i> .....	419
<i>Describe Cloud Infrastructure and Operations</i> .....	422
<i>Compute Virtualization (Containers and Virtual Machines)</i> .....	422
<i>Installing Docker</i> .....	424
<i>Using Docker Commands</i> .....	425
<i>Connectivity (Virtual Switches, SD-WAN and SD-Access)</i> .....	426
<i>Virtual Switches</i> .....	427
<i>Virtual Machine Device Queues (VMDq)</i> .....	428
<i>Single Root IO Virtualization (SR-IOV)</i> .....	429
<i>SD-WAN and SD-Access</i> .....	429
<i>Cisco SD-WAN Solution (formerly Viptela)</i> .....	430
<i>Software-Defined Access (or SD-Access)</i> .....	434
<i>Virtualization Functions (NFVI, VNF, and L4/L1)</i> .....	437
<i>NFVI and VNFs</i> .....	437
<i>Virtual Topology Forwarder (VTF)</i> .....	438
<i>Automation and Orchestration Tools (CloudCenter, DNA-center, and Kubernetes)</i> .....	441
<i>Cisco CloudCenter Manager and Orchestrator</i> .....	441
<i>Cisco DNA Center</i> .....	442
<i>Kubernetes</i> .....	444
<i>Exam Essentials</i> .....	457
<i>Further Reading</i> .....	458
Chapter 7: Network Programmability.....	460
<i>Describe Architectural and Operational Considerations for a Programmable Network</i> .....	460
<i>Data Models and Structures (YANG, JSON and XML)</i> .....	460
<i>YANG</i> .....	461
<i>YAML</i> .....	464
<i>JSON</i> .....	465
<i>JSON Example</i> .....	465

XML .....	466
XML Example .....	466
Device Programmability (gRPC, NETCONF and RESTCONF) .....	467
gRPC.....	467
NETCONF.....	469
NETCONF Example .....	470
RESTCONF .....	471
Using RESTCONF to Retrieve Full Running Configuration.....	471
Using RESTCONF to Retrieve Interface Specific Attributes .....	472
Controller Based Network Design (Policy Driven Configuration and Northbound/Southbound APIs) ..	472
Policy-driven Configuration .....	472
Northbound and Southbound APIs .....	473
Configuration Management Tools (Agent and Agentless) and Version Control Systems (Git and SVN) .....	474
Configuration Management Tools (Agent and Agentless) .....	474
Version Control Systems (Git and SVN).....	476
Creating Configuration Change .....	479
Building New Configuration.....	479
Testing New Configuration .....	480
Deploying New Configuration.....	480
Exam Essentials.....	487
Further Reading .....	488
Chapter 8: Internet of Things.....	490
Describe Architectural Framework and Deployment Considerations for Internet of Things (IoT) .....	490
IoT Technology Stack (IoT Network Hierarchy, Data Acquisition and Flow) .....	493
Embedded Systems Layer .....	493
Multi-Service Edge (or Access) Layer .....	494
Core Network Layer .....	494
Data Center Cloud Layer.....	494
Data Acquisition and Flow.....	495
IoT Standards and Protocols (characteristics within IT and OT environment) .....	496
IoT Security (network segmentation, device profiling, and secure remote access).....	498
IoT Edge and Fog Computing (data aggregation and edge intelligence).....	499
Data Aggregation .....	500
Edge Intelligence.....	501
Exam Essentials.....	502
Further Reading .....	503

SAMPLE GUIDE

FULL GUIDE HAS 500+ PAGES.

## Preface

Congratulations! You have taken your first step towards passing the CCIE Security 400-251 V5.0 written exam.

This study guide is dedicated to *all those souls who will never settle for less than they can be, do, share, and give!*

## CCIE Security v5.0 Hardware and Software

### Virtual Machines

- Security Appliances
  - Cisco Identity Services Engine (ISE): 2.1.0
  - Cisco Secure Access Control System (ACS): 5.8.0.32
  - Cisco Web Security Appliance (WSA): 9.2.0
  - Cisco Email Security Appliance (ESA): 9.7.1
  - Cisco Wireless Controller (WLC): 8.0.133
  - Cisco Firepower Management Center Virtual Appliance: 6.0.1 and/or 6.1
  - Cisco Firepower NGIPSv: 6.0.1
  - Cisco Firepower Threat Defense: 6.0.1
- Core Devices
  - IOSv L2: 15.2
  - IOSv L3: 15.5(2)T
  - Cisco CSR 1000V Series Cloud Services Router: 3.16.02.S
  - Cisco Adaptive Security Virtual Appliance (ASAv): 9.6.1
- Others
  - Test PC: Microsoft Windows 7
  - Active Directory: Microsoft Windows Server 2008 (AD is not required to be configured by the candidate)
  - Cisco Application Policy Infrastructure Controller Enterprise Module : 1.2
  - Cisco Unified Communications Manager: (The CUCM is not required to be configured by the candidate)
  - FireAMP Private Cloud
  - AnyConnect 4.2

### Physical Devices

- Cisco Catalyst Switch: C3850-12S 16.2.1
- Cisco Adaptive Security Appliance: 5512-X: 9.6.1
- Cisco 2504 Wireless Controller: 2504: 8.0.133.0
- Cisco Aironet: 1602E: 15.3.3-JC
- Cisco Unified IP Phone: 7965: 9.2(3) (IP Phone is not required to be configured by the candidate)

### Topics Added in CCIE Security v5.0 (versus V4.1)

- Advanced Threat Protection
- Virtualization
- Automation
- Information Exchange
- Evolving Technologies

### Topics Removed in CCIE Security v5.0 (versus V4.1)

- Legacy IPS Appliance
- Easy VPN

CCIE Security V5.0 Blueprint Domains	Domain Description	Written Exam %
Perimeter Security and Intrusion Prevention	Cisco FirePOWER, Cisco ASA, Cisco IOS ZBFW, DDoS Mitigation	21%
Advanced Threat Protection and Content Security	AMP Solutions and Security Protocols	17%
Secure Connectivity and Segmentation	IKE/IPSec, TrustSec, GETVPN, DMVPN, FlexVPN, Security protocols and algorithms	17%
Identity Management, Information Exchange, and Access Control	ISE, RADIUS/TACACS+, WLAN Security and Protocols	22%
Infrastructure Security, Virtualization, and Automation	Attacks, Cisco ACI, standard bodies, Cisco DNA/SAFE, NetFlow, ACLs etc.	13%
Evolving Technologies	Cloud, SDN, IoT	10%

It is exciting to see that Cisco has aggressively updated the exam blueprint to keep pace with the changes taking place in the security and networking industries. Following are worth noting:

- As we know, Cisco is an acquisition machine and recently snapped up Lancope (NBA/NetFlow), OpenDNS (cloud-delivered security), and SourceFire (FirePower product line) security companies. Both newly acquired and organically built (ex. ACI) products and solutions are now part of the new CCIE Security blueprint (v5.0)
- Overall exam blueprint now seems more consolidated (8 versus 6 exam sections)

- Identity Management, Information Exchange, and Access Control is the largest content contributor to the exam now (22% and 24% of the written and lab exams respectively)
- Security infrastructure products for perimeter security and intrusion prevention is the second largest content area when it comes written and lab exam content (21% and 23% of the written and lab exams respectively)
- It seems finally all of the VPN content is now consolidated into Secure Connectivity and Segmentation area (17% and 19% of the written and lab exams respectively)
- Infrastructure Security, Virtualization, and Automation now includes Cisco ACI and virtualized security domain
- There is no change to Evolving Technologies section across v4.1 and v5.0 exam blueprint. It continues to include SDN, Cloud and Internet of Things (IoT)
- Last but not least, Cisco also seems to be stepping up on transparency around the CCIE exam content with a lot of details for each section.

### What this Exam Cert Guide Covers

As you may already have noticed on the "Contents at a Glance" page that this guide has been formatted around the Cisco's official CCIE 400-251 V5.0 exam topics or [curriculum](#). So as you read through the chapters, you will know exactly where you're within your learning journey.

All contents are carefully compiled and covered in enough details however still trimmed to exactly what's necessary to pass the exam. Each exam topic has "Further Reading" section where we have done the research for you in the form of curated set of links. You can refer to them if you are looking for more in-depth details or want to refer to the source of the original text.

### How to Use this Exam Cert Guide

This guide is for anyone who's studying for CCIE Security written 400-251 V5.0 exam, regardless if this is your first time sitting for a CCIE written exam or you're a pro who's recertifying. We strongly suggest to take a methodical approach for exam preparation, i.e. start with a target date when you would like to sit for the actual exam and then work backwards to see what kind of study plan would work for you. We believe you can cover the entire contents within eight weeks including the practice questions (available on our [website](#)). We strongly suggest you to also use other study resources in addition to bringing your prior experience to bear in order to successfully pass the exam.

If you're totally in a crunch and consider yourself an advanced learner, you could try your luck by skimming through the "Exam Essentials" sections for each chapter- We guarantee you that you will be better prepared to tackle the exam with them than without!

### What's Available on the CCIEin8Weeks Website

**FULL GUIDE HAS 500+ PAGES.**

CCIEin8Weeks.com carries the extras (sold separately) that go hand in hand with this study guide to further ensure your exam success!

- Six practice exams (one for each section as per official curriculum), One final exam
- Four study plans, to help you track your progress or help you come up with your own plan
- CCIE Exam community forum, to help you interact with others, share knowledge, find study partners etc.
- ExamSkope™ to help you keep up to speed on the buzz around CCIE Security V5 written exam

SAMPLE GUIDE



## Chapter 1: Perimeter Security and Intrusion Prevention

This chapter covers the following exam topics from Cisco's official 400-251 V5.0 written exam curriculum.

- Describe, implement, and troubleshoot HA features on Cisco ASA and Cisco FirePOWER Threat Defense (FTD)
- Describe, implement, and troubleshoot clustering on Cisco ASA and Cisco FTD
- Describe, implement, troubleshoot, and secure routing protocols on Cisco ASA and Cisco FTD
- Describe, implement, and troubleshoot different deployment modes such as routed, transparent, single, and multi-context on Cisco ASA and Cisco FTD
- Describe, implement, and troubleshoot firewall features such as NAT (v4,v6), PAT, application inspection, traffic zones, policy-based routing, traffic redirection to service modules, and identity firewall on Cisco ASA and Cisco FTD
- Describe, implement, and troubleshoot IOS security features such as Zone-Based Firewall (ZBF), application layer inspection, NAT (v4,v6), PAT and TCP intercept on Cisco IOS/IOS-XE
- Describe, implement, optimize, and troubleshoot policies and rules for traffic control on Cisco ASA, Cisco FirePOWER and Cisco FTD
- Describe, implement, and troubleshoot Cisco Firepower Management Center (FMC) features such as alerting, logging, and reporting
- Describe, implement, and troubleshoot correlation and remediation rules on Cisco FMC
- Describe, implement, and troubleshoot Cisco FirePOWER and Cisco FTD deployment such as in-line, passive, and TAP modes
- Describe, implement, and troubleshoot Next Generation Firewall (NGFW) features such as SSL inspection, user identity, geolocation, and AVC (Firepower appliance)
- Describe, detect, and mitigate common types of attacks such as DoS/DDoS, evasion techniques, spoofing, man-in-the-middle, and botnet

## Chapter 1: Perimeter Security and Intrusion Prevention

Cisco continues to be in the process of integrating the acquired FirePower product lines (from SourceFire) to existing ASA legacy firewall product line. Over the last two years, Cisco has been adding Firepower features to the ASA product line. In September 2014, Cisco added Firepower services from Sourcefire to Cisco ASA firewalls. With the new Firepower NGFW, an existing ASA 5500 can be upgraded via software to the new image. Additionally, some of the older Firepower appliances can now also be upgraded to the new image.

The core of the Firepower NGFW is a new Linux operating system distribution dubbed as FXOS (Firepower eXtensible Operating System). The new FXOS introduces service-chaining capabilities that can help to enable a security inspection and remediation workflow. Chaining and understanding context is further enhanced through the integration of the Cisco Identity Service Engine (ISE). Firepower can now consume Cisco ISE information about users and policy. Additionally, the integration of ISE and Firepower enables rapid threat containment where an alert from Firepower can be extended through ISE to keep a threat or malicious end point off the network.

The Firepower Threat Defense appliance provides a unified next-generation firewall and next-generation IPS device. In addition to the IPS features available on Firepower Software models, firewall and platform features include Site-to-Site VPN, robust routing, NAT, clustering (for the Firepower 9300), and other optimizations in application inspection and access control.

The Firepower Threat Defense software is supported on the following platforms:

- Firepower 9300
- Firepower 4100 series
- ASA 5512-X through 5555-X
- ASA 5508-X and 5516-X
- ASA 5506-X series

As you go through the sections below, please note that a lot of the features and system behaviors apply across legacy ASA and new integrated platform running FXOS. However, not all ASA features are available in FXOS at the time of writing this text.

### Further Reading

You can read up on current state of integration and ASA versus FXOS compatibility below.

<https://goo.gl/ZRRO75>

## Describe, implement, and troubleshoot HA features on Cisco ASA

Configuring high availability requires two identical ASAs connected to each other through a dedicated failover link and, optionally, a Stateful Failover link. The health of the active interfaces and units is monitored to determine if specific failover conditions are met. If those conditions are met, failover occurs.

The ASA supports two failover configurations, Active/Active failover and Active/Standby failover. Each failover configuration has its own method for determining and performing failover. With Active/Active failover, both units can pass network traffic. This also lets you configure traffic sharing on your network. Active/Active failover is available only on units running in multiple context mode. With Active/Standby failover, only one unit passes traffic while the other unit waits in a standby state. Active/Standby failover is available on units running in either single or multiple context mode. Both failover configurations support stateful or stateless (regular) failover. When the security appliance is configured for Active/Active stateful failover, you cannot enable IPsec or SSL VPN. Therefore, these features are unavailable. VPN failover is available for Active/Standby failover configurations only.

### Failover System Requirements

This section describes the hardware, software, and license requirements for ASAs in a failover configuration.

#### Hardware Requirements

The two units in a failover configuration must be the same model, have the same number and types of interfaces, and the same SSMs installed (if any). Both units must have the same amount of RAM memory installed. If you are using units with different Flash memory sizes in your failover configuration, make sure the unit with the smaller Flash memory has enough space to accommodate the software image files and the configuration files. If it does not, configuration synchronization from the unit with the larger Flash memory to the unit with the smaller Flash memory will fail.

#### Software Requirements

The two units in a failover configuration must be in the same operating modes (routed or transparent, single or multiple context). They must have the same major (first number) and minor (second number) software version. However, you can use different versions of the software during an upgrade process; for example, you can upgrade one unit from Version 7.0(1) to Version 7.0(2) and have failover remain active. We recommend upgrading both units to the same version to ensure long-term compatibility.

## Licensing Requirements

The licensed features (such as SSL VPN peers or security contexts, for example) on both units participating in failover must be identical.

## Failover and Stateful Failover Links

This section describes the failover and the Stateful Failover links, which are dedicated connections between the two units in a failover configuration.

### Failover Link

The two units in a failover pair constantly communicate over a failover link to determine the operating status of each unit. The following information is communicated over the failover link:

- The unit state (active or standby)
- Hello messages (keep-alives)
- Network link status
- MAC address exchange
- Configuration replication and synchronization

All information sent over the failover and Stateful Failover links is sent in clear text unless you secure the communication with a failover key. If the ASA is used to terminate VPN tunnels, this information includes any usernames, passwords and preshared keys used for establishing the tunnels. Transmitting this sensitive data in clear text could pose a significant security risk. We recommend securing the failover communication with a failover key if you are using the ASA to terminate VPN tunnels.

You can use any unused Ethernet interface on the device as the failover link; however, you cannot specify an interface that is currently configured with a name. The LAN failover link interface is not configured as a normal networking interface; it exists for failover communication only. This interface should only be used for the LAN failover link (and optionally for the Stateful Failover link).

Connect the LAN failover link in one of the following two ways:

- Using a switch, with no other device on the same network segment (broadcast domain or VLAN) as the LAN failover interfaces of the ASA.
- Using a crossover Ethernet cable to connect the appliances directly, without the need for an external switch.

When you use a crossover cable for the LAN failover link, if the LAN interface fails, the link is brought down on both peers. This condition may hamper troubleshooting efforts because you cannot easily determine which interface failed and caused the link to come down.

### Stateful Failover Link

To use Stateful Failover, you must configure a Stateful Failover link to pass all state information. You have three options for configuring a Stateful Failover link:

- You can use a dedicated Ethernet interface for the Stateful Failover link.
- If you are using LAN-based failover, you can share the failover link.
- You can share a regular data interface, such as the inside interface. However, this option is not recommended.

If you are using a dedicated Ethernet interface for the Stateful Failover link, you can use either a switch or a crossover cable to directly connect the units. If you use a switch, no other hosts or routers should be on this link. Be sure to enable the PortFast option on Cisco switch ports that connect directly to the ASA. If you use a data interface as the Stateful Failover link, you receive the following warning when you specify that interface as the Stateful Failover link:

```
***** WARNING ***** WARNING ***** WARNING ***** WARNING *****
Sharing Stateful failover interface with regular data interface is not a recommended
configuration due to performance and security concerns.
***** WARNING ***** WARNING ***** WARNING ***** WARNING *****
```

Sharing a data interface with the Stateful Failover interface can leave you vulnerable to replay attacks. Additionally, large amounts of Stateful Failover traffic may be sent on the interface, causing performance problems on that network segment. Using a data interface as the Stateful Failover interface is supported in single context, routed mode only.

In multiple context mode, the Stateful Failover link resides in the system context. This interface and the failover interface are the only interfaces in the system context. All other interfaces are allocated to and configured from within security contexts.

The IP address and MAC address for the Stateful Failover link does not change at failover unless the Stateful Failover link is configured on a regular data interface.

All information sent over the failover and Stateful Failover links is sent in clear text unless you secure the communication with a failover key. If the ASA is used to terminate VPN tunnels, this information includes any usernames, passwords, and preshared keys used for establishing the tunnels. Transmitting this sensitive data in clear text could pose a significant security risk. We recommend securing the failover communication with a failover key if you are using the ASA to terminate VPN tunnels.

### Failover Interface Speed for Stateful Links

If you use the failover link as the Stateful Failover link, you should use the fastest Ethernet interface available. If you experience performance problems on that interface, consider dedicating a separate interface for the Stateful Failover interface.

Use the following failover interface speed guidelines for the adaptive security appliances:

- Cisco ASA 5510
  - Stateful link speed can be 100 Mbps, even though the data interface can operate at 1 Gigabit due to the CPU speed limitation.
- Cisco ASA 5520/5540/5550
  - Stateful link speed should match the fastest data link.
- Cisco ASA 5580/5585

– Use only non-management 1 Gigabit ports for the stateful link because management ports have lower performance and cannot meet the performance requirement for stateful failover. For optimum performance when using long distance LAN failover, the latency for the failover link should be less than 10 milliseconds and no more than 250 milliseconds. If latency is more than 10 milliseconds, some performance degradation occurs due to retransmission of failover messages.

All platforms support sharing of failover heartbeat and stateful link, but we recommend using a separate heartbeat link on systems with high Stateful Failover traffic.

### **Avoiding Interrupted Failover Links**

Because adaptive security appliances use failover LAN interfaces to transport messages between primary and secondary units, if a failover LAN interface is down (that is, the physical link is down or the switch used to connect the LAN interface is down), then the adaptive security appliance failover operation is affected until the health of the failover LAN interface is restored. If all communication is cut off between the units in a failover pair, both units go into the active state, which is expected behavior. When communication is restored and the two active units resume communication through the failover link or through any monitored interface, the primary unit remains active, and the secondary unit immediately returns to the standby state. This relationship is established regardless of the health of the primary unit.

Because of this behavior, stateful flows that were passed properly by the secondary active unit during the network split are now interrupted. To avoid this interruption, failover links and data interfaces should travel through different paths to decrease the chance that all links fail at the same time. If only one failover link is down, the adaptive security appliance takes a sample of the interface health, exchanges this information with its peer through the data interface, and performs a switchover if the active unit has a greater number of down interfaces. Subsequently, the failover operation is suspended until the health of the failover link is restored.

### **Active/Active and Active/Standby Failover**

Two types of failover configurations are supported by the ASA: Active/Standby and Active/Active. In Active/Standby failover, one unit is the active unit. It passes traffic. The standby unit does not actively pass traffic. When a failover occurs, the active unit fails over to the standby unit, which then becomes active. You can use Active/Standby failover for ASAs in single or multiple context mode, although it is most commonly used for ASAs in single context mode.

Active/Active failover is only available to ASAs in multiple context mode. In an Active/Active failover configuration, both ASAs can pass network traffic. In Active/Active failover, you divide the security contexts on the ASA into failover groups. A failover group is simply a logical group of one or more security contexts. Each group is assigned to be active on a specific ASA in the failover pair. When a failover occurs, it occurs at the failover group level.

## Determining Which Type of Failover to Use

The type of failover you choose depends upon your ASA configuration and how you plan to use the ASAs.

If you are running the ASA in single mode, then you can use only Active/Standby failover.

Active/Active failover is only available to ASAs running in multiple context mode.

If you are running the ASA in multiple context mode, then you can configure either Active/Active failover or Active/Standby failover.

- To allow both members of the failover pair to share the traffic, use Active/Active failover. Do not exceed 50% load on each device.
- If you do not want to share the traffic in this way, use Active/Standby or Active/Active failover.

Feature	Active/Active	Active/Standby
Single Context Mode	No	Yes
Multiple Context Mode	Yes	Yes
Traffic Sharing Network Configurations	Yes	No
Unit Failover	Yes	Yes
Failover of Groups of Contexts	Yes	No
Failover of Individual Contexts	No	No

## Stateless (Regular) and Stateful Failover

The ASA supports two types of failover, regular and stateful. This section includes the following topics:

### Stateless Failover

When a failover occurs, all active connections are dropped. Clients need to reestablish connections when the new active unit takes over.

### Stateful Failover

When Stateful Failover is enabled, the active unit continually passes per-connection state information to the standby unit. After a failover occurs, the same connection information is available at the new active unit. Supported end-user applications are not required to reconnect to keep the same communication session.

State Information Passed to Standby Unit	State Information Not Passed to Standby Unit
NAT translation table	The HTTP connection table (unless HTTP replication is enabled).
TCP connection states	The user authentication (uauth) table.



	Inspected protocols are subject to advanced TCP-state tracking, and the TCP state of these connections is not automatically replicated. While these connections are replicated to the standby unit, there is a best-effort attempt to re-establish a TCP state.
UDP connection states	The routing tables. After a failover occurs, some packets may be lost or routed out of the wrong interface (the default route) while the dynamic routing protocols rediscover routes.
The ARP table	State information for Security Service Modules.
The Layer 2 bridge table (when running in transparent firewall mode)	DHCP server address leases.
The HTTP connection states (if HTTP replication is enabled)	Stateful failover for phone proxy. When the active unit goes down, the call fails, media stops flowing, and the phone should unregister from the failed unit and re register with the active unit. The call must be re-established.
The ISAKMP and IPsec SA table	—
GTP PDP connection database	—
SIP signalling sessions	—

For VPN failover, VPN end-users should not have to reauthenticate or reconnect the VPN session in the event of a failover. However, applications operating over the VPN connection could lose packets during the failover process and not recover from the packet loss.

### Transparent Firewall Mode Requirements

When the active unit fails over to the standby unit, the connected switch port running Spanning Tree Protocol (STP) can go into a blocking state for 30 to 50 seconds when it senses the topology change. To avoid traffic loss while the port is in a blocking state, you can configure one of the following workarounds depending on the switch port mode:

- Access mode—Enable the STP PortFast feature on the switch:

```
interface interface_id
spanning-tree portfast
```

The PortFast feature immediately transitions the port into STP forwarding mode upon linkup. The port still participates in STP. So if the port is to be a part of the loop, the port eventually transitions into STP blocking mode.

- Trunk mode—Block BPDUs on the ASA on both the inside and outside interfaces:

```
access-list id ethertype deny bpdu
access-group id in interface inside_name
access-group id in interface outside_name
```

Blocking BPDUs disables STP on the switch. Be sure not to have any loops involving the ASA in your network layout.

If neither of the above options are possible, then you can use one of the following less desirable workarounds that impacts failover functionality or STP stability:

- Disable failover interface monitoring.
- Increase failover interface holdtime to a high value that will allow STP to converge before the ASAs fail over.
- Decrease STP timers to allow STP to converge faster than the failover interface holdtime.

SAMPLE GUIDE