# Aruba Certified Network Security Associate
## OFFICIAL CERTIFICATION STUDY GUIDE
## (EXAM HPE6-A78)

**First Edition**

**Miriam Allred**

HPE Press
660 4th Street, #802
San Francisco, CA 94107

**Aruba Certified Network Security Associate**
**Official Certification Study Guide (Exam HPE6-A78)**
Miriam Allred

© 2020 Hewlett Packard Enterprise Development LP.

Published by:

Hewlett Packard Enterprise Press
660 4th Street, #802
San Francisco, CA 94107

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

ISBN: **978-1-7360155-0-6**

**WARNING AND DISCLAIMER**
This book provides information about the topics covered in the Aruba Certified Network Security Associate (HPE6-A78) certification exam. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an "as is" basis. The author, and Hewlett Packard Enterprise Press, shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the author and are not necessarily those of Hewlett Packard Enterprise Press.

**FEEDBACK INFORMATION**

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

Readers' feedback is a continuation of the 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 hpepress@epac.com. Please make sure to include the book title and ISBN in your message.

We appreciate your feedback.

**Publisher**: Hewlett Packard Enterprise Press

**HPE Contributors**: Darren Crawford, Herman Robers, Kelly Kutz

**HPE Press Program Manager**: Michael Bishop

## About the Author

Miriam Allred has spent the last 15 years configuring, testing, and troubleshooting wired and wireless networks. Miriam combines this wide range of technical expertise with pedagogy and instructional design training, allowing her to create technical training courses for both advanced and entry-level networking professionals. Miriam Allred has a Master's degree from Cleveland State University and a Bachelor's degree from Brigham Young University.

## Introduction

This book is based on the *Aruba Networks Security Fundamentals*, Rev 20.41 course. It helps you prepare for the HPE6-A78 exam, a prerequisite for becoming an Aruba Certified Security Associate. The exam validates candidates' knowledge, skills, and ability to describe common security threats and vulnerabilities.

This guide provides an overview of foundational security technologies. Learn how to create a trusted network infrastructure with Aruba mobility solutions and switches. In addition to covering topics such as device hardening, the guide discusses implementing security at the edge with AAA, basic roles and firewall policies, dynamic segmentation, and endpoint classification. You will also learn about basic threat detection technologies and how to collect logs and alarms and use them to initiate an investigation.

## Certification and Learning

Hewlett Packard Enterprise Certification and Learning provides end-to-end continuous learning programs and professional certifications that can help you open doors and accelerate your career.

We provide

– **Professional sales and technical training and certifications** to give you the critical skills needed to design, manage, and implement the most sought-after IT disciplines;

– **Continuous learning activities and job-role based learning plans** to help you keep pace with the demands of the dynamic, fast-paced IT industry; and

– **Advanced training** to help you navigate and seize opportunities within the top IT transformation areas that enable business advantage today.

As a Certification and Learning certified member, your skills, knowledge, and real-world experience are recognized and valued in the marketplace. To continue your professional and career growth, you have access to our large HPE community of world-class IT professionals, trend-makers and decision-makers. Share ideas, best practices, business insights, and challenges as you gain professional connections globally.

To learn more about HPE Certification and Learning certifications and continuous learning programs, please visit http://certification-learning.hpe.com

## Audience

This book is designed for network engineers or help desk engineers with six months to one year of experience, working in either a corporate or Aruba partner environment.

## Assumed Knowledge

Aruba Certified Network Security Associate is an entry-level security book, but it assumes that you have fundamental knowledge in wireless technologies and Ethernet switching.

## Minimum Qualifications

It is assumed that you have worked at least six months to a year in networking and have a basic understanding of wired and wireless networks, as well as of Aruba switches and mobility solutions. You should have an interest in learning about how to improve network security.

## Relevant Certifications

After you pass these exams, your achievement may be applicable toward more than one certification. To determine which certifications can be credited with this achievement, log in to The Learning Center and view the certifications listed on the exam's More Details tab. You might be on your way to achieving additional certifications.

## Preparing for Exam HPE6-A78

This self-study guide does not guarantee that you will have all the knowledge you need to pass the exam. It is expected that you will also draw on real-world experience and would benefit from completing the hands-on lab activities provided in the instructor-led training. To pass the certification exam, you should be able to describe common security threats and vulnerabilities. The exam also tests a candidate's knowledge of device hardening, implementation of security at the edge with AAA, basic roles and firewall policies, dynamic segmentation, and endpoint classification. It covers basic threat detection technologies, collecting logs and alarms.

## Recommended HPE Training

Recommended training to prepare for each exam is accessible from the exam's page in The Learning Center. See the exam attachment, "Supporting courses," to view and register for the courses.

## Obtain Hands-on Experience

You are not required to take the recommended, supported courses, and completion of training does not guarantee that you will pass the exams. Hewlett Packard Enterprise strongly recommends a combination of training, thorough review of courseware and additional study references, and sufficient on-the-job experience prior to taking an exam.

## Exam Registration

To register for an exam, go to https://certification-learning.hpe.com/tr/learn_more_about_exams.html

# CONTENTS

1 Security Threats and the Aruba Security Strategy........................1

Assumed Knowledge........................1

Overview........................1

Confidentiality, Integrity, and Availability (CIA)........................1

Threat Overview........................2

Threats........................2

Vulnerabilities versus Threats........................2

Actors........................4

Meet Alice, Bob, Eve, and Mallory........................4

What Is Malware?........................5

Malware: How It Infects a System........................5

Malware: What It Does........................7

Denial of Service (DoS)........................10

Distributed Denial of Service (DDoS)........................11

Eavesdropping........................12

Network Reconnaissance........................13

Man-in-the-Middle (MITM) Attack........................15

Some Methods for Launching MITM Attacks........................16

Address Resolution Protocol (ARP) Review........................17

Using ARP Poisoning to Implement an MITM Attack........................17

MAC and IP Spoofing........................19

Email Spoofing and Phishing........................20

Social Engineering........................21

Best Practices for Avoiding Social Engineering Attacks........................21

Additional Attacks against Passwords........................22

How to Protect against Password-based Attacks?........................23

Attack Stages........................24

Kill Chain........................24

Targeted Attacks versus Opportunistic Attacks........................25

Targeted Attacks: Reconnaissance........................25

Targeted Attacks: Weaponization and Delivery........................27

Targeted Attacks: Exploitation to Actions on Objective........................28

Opportunistic Attack Chains........................29

Lateral Movement........................30

Need for Zero Trust........................31

Aruba Security Strategy....32
Industry Analysts on ZTN and ZTNA....32
Aruba 360 Secure Fabric....33
Create a Trusted Network Infrastructure....34
Enforce Micro-Segmentation....35
Log and Inspect within the Trusted Network Infrastructure....36
Continuously Monitor, Control, and Orchestrate with the Aruba 360 Security Exchange....37
Implement Same Security Everywhere....38
Summary....39
Learning Check....40

2 Security Technologies....41
Assumed Knowledge....41
Overview....41
Regulatory Compliance....41
Regulatory Requirements....41
PCI DSS 3.2 Requirements....43
Understand Your Company's Policies....44
Secure Communications: Symmetric Encryption and Hash-based Authentication....44
Goals of Secure Communications....44
Using Encryption for Data Privacy....46
Decryption....46
What Goes into Encryption/Decryption?....47
Simple Example of an Algorithm: Caesar Cipher....48
Symmetric Encryption....48
A Simple Example of a Symmetric Key Algorithm: XOR....49
Stream Algorithms....50
Block Algorithms....51
The Risks of Key Reuse with Symmetric Algorithms....52
Initialization Vectors (IVs)....54
The Importance of Key Length....54
Hash Algorithms....55
Hash-based Message Authentication Codes (HMAC)....56
Other Ways to Authenticate Messages....57
How Do Parties Communicate the Symmetric Keys?....58
Diffie-Hellman (DH) for Secure Key Agreement....59
Diffie-Hellman Susceptibility to MITM....60
NIST Suite B and CNSA....61
Recommendations for Algorithms....61

Secure Communications: Asymmetric Encryption, Certificates, and PKI....... 62
- Asymmetric (Public Key) Encryption.................................................62
- Asymmetric Encryption for Data Signing..........................................63
- Recommendations for Data Signature Algorithms .............................64
- Asymmetric Encryption Considerations ............................................64
- What is a Digital or X.509 Certificate? ............................................65
- What Do You Use Certificates for?...................................................66
- Example Certificate ..........................................................................67
- Subject Names .................................................................................68
- CAs and the Public Key Infrastructure (PKI)........................................69
- Certificate Signing ...........................................................................71
- Chain of Trust ..................................................................................71
- Validating Certificates and the Chain of Trust ...................................72
- What Does It Mean for a Root CA Certificate to Be Trusted? ...............74
- What Else Is Required for a Certificate to Be Valid? ...........................75
- Certificate Validation in Web Browsers .............................................76
- Public CAs versus Private CAs.........................................................78
- Self-Signed Certificates....................................................................79
- Online versus Offline Keypair and Certificate Signing Request (CSR) Generation................................................................80
- Creating Certificate Signing Requests (CSRs) and Keypairs.................80
- Obtaining Certificates .......................................................................81
- Certificate File Formats ....................................................................82
- Installing Certificates .......................................................................83

Secure Communications: Transport Layer Security (TLS) ...........................84
- Transport Layer Security (TLS)..........................................................84
- Introducing TLS v1.3 ........................................................................85

Authentication, Authorization, and Accounting (AAA) .............................85
- AAA Roles .......................................................................................86
- High-Level Overview of RADIUS Authentication/ Authorization Process...........................................................................87
- RADIUS Authentication Methods ......................................................88
- RADIUS Packets and AVPs ...............................................................90
- AVP Role in Decisions.......................................................................91
- RADIUS Accounting .........................................................................92
- RADIUS Security Considerations ......................................................93
- RadSec ............................................................................................94
- TACACS+.........................................................................................95
- RADIUS vs TACACS+ .........................................................................96

Summary.................................................................................................97

Learning Check........................................................................................98

3 Hardening Switches....................101
Assumed Knowledge....................101
Overview....................101
Hardening Overview....................101
Why Harden Devices?....................101
Best Practices Checklist....................102
Out-of-Band Management....................102
Network Infrastructure Device Planes....................102
Out-of-Band Management to a Console Port....................103
In-Band Management....................104
Ethernet Out-of-Band Management....................105
CLI Commands: Management Interface Configuration....................107
CLI Commands: Locking Down Protocols to the Out-of-Band Management Network....................107
ArubaOS-Switch: Management VLAN....................108
Methods for Restricting In-Band Management Access....................109
Secure Manager Authentication....................110
Best Practices for Authentication Methods....................110
Manager Roles....................111
Enforcing Best Practices for Local Authentication....................112
CLI Commands: Local Authentication Configuration....................113
Understanding How Credentials Are Stored in the Config....................114
Setting up External Authentication for Management Access....................115
Specifying the External Server....................115
Specifying External Access Methods....................117
Using RADIUS AVPs to Assign Manager Roles on an ArubaOS-Switch....................119
Using TACACS+ Privilege Levels to Assign Manager Roles on an ArubaOS-Switch....................120
Using Aruba VSA to Assign Manager Roles (RADIUS or TACACS) on an AOS-CX Switch....................124
Order of Priority for AVPs/VSAs on AOS-CX....................124
CLI Commands: TACACS+ Authentication Configuration....................125
Secure Protocols....................126
Use Secure Protocols....................126
Set Up SSH Securely....................128
CLI Commands: SSH Configuration....................129
Set Up Management Stations to Trust the Switch Public Keys....................130
Set Up Secure Access to the Web UI....................134
Managing Certificates on Aruba Switches....................135

CLI Commands: Certificate Management ........................................136
Managing Certificates with Enrollment over Secure Transport (EST) ........................................137
Setting up EST ........................................137
Disable SNMPv1/v2 ........................................138
ArubaOS-Switch Set Up SNMPv3 ........................................139
AOS-CX: Set Up SNMPv3 ........................................141
CLI Commands: SNMPv3 Configuration........................................141
Physical Security and Other Measures ........................................142
Ensure Physical Security ........................................142
Enable Control Plane Policing (CoPP)........................................143
Enable Enhanced Secure Mode........................................144
CLI Commands: CoPP and Enhanced Secure Mode........................................145
Authenticated Network Time Protocol (NTP) ........................................146
CLI Commands: Authenticated NTP Setup ........................................147
Take Additional Hardening Actions ........................................147
Understand the Trusted Platform Module (TPM)........................................149
Summary........................................150
Learning Check........................................150

**4 Hardening the ArubaOS........................................153**
Assumed Knowledge........................................153
Overview ........................................153
Introduction ........................................153
Why Harden the Wireless Infrastructure Devices........................................153
Best Practices Checklist........................................154
Determine Requirements for FIPS Compliance........................................155
FIPS/TAA Hardware and Software........................................155
Lock Down Administrative Access........................................155
Best Practices Checklist........................................155
Protect the Console Port........................................156
ArubaOS Control Plane vs Datapath ........................................157
Adjust the Control Plane ACL (Firewall ACL Whitelist) ........................................158
Secure Manager Access to the ArubaOS Web UI ........................................160
Create the Authentication Group........................................161
Create the Authentication Server........................................161
How the External Authentication Server Assigns Managers to Roles ........................................162
Management Roles ........................................166
Configure Admin Authentication Settings ........................................166

MC Certificate Management ........ 167
Installing a Trusted CA Certificate through the ArubaOS UI ........ 168
Methods for Obtaining Server Certificates on an MC ........ 169
Using EST on MCs ........ 173
Using a Server Certificate for the ArubaOS Web UI ........ 174
Use Certificate-based Authentication for the Web UI ........ 175
Process of Certificate-based Authentication for Web UI ........ 177
"Disable" Local Authentication with Random Password ........ 177
Lock Down Services ........ 178
Best Practices Checklist ........ 178
SNMPv3 on ArubaOS Devices ........ 179
Using SNMPv3 ........ 180
Setting up Authenticated NTP ........ 181
Control Plane Defense ........ 185
Implement Global Firewall Settings ........ 186
Enforce DHCP ........ 188
Secure ArubaOS Device-to-Device Communications ........ 189
Why CPsec ........ 189
CPsec Settings ........ 190
Secure End-to-End Communications ........ 191
ArubaOS TPMs ........ 193
Obtain More Information ........ 193
Summary ........ 194
Learning Check ........ 194

**5 Secure LAN Protocols ........ 195**
Assumed Knowledge ........ 195
Overview ........ 195
Implement Spanning Tree Protections ........ 196
Spanning Tree Normal Operation ........ 196
Spanning Tree Vulnerability: Rogue Device Becomes Root Bridge ........ 197
BPDU Protection ........ 198
Root Guard ........ 199
CoPP on Spanning Tree or BPDU Throttling ........ 200
Summary of Spanning Tree Protections ........ 201
CLI Commands: Configuration of Spanning Tree Protections ........ 201
Use DHCP Snooping and ARP Protection ........ 202
DHCP Review ........ 202
DHCP Attacks ........ 203

ArubaOS-Switch: Using DHCP Snooping to Protect against DHCP Attacks ........ 203
ArubaOS-Switch: Authorized Servers ........ 205
ArubaOS-Switch: Filtering Option 82 from Connected Devices ........ 208
Review ARP Snooping and Poisoning ........ 209
ArubaOS-Switch: ARP Protection ........ 210
ArubaOS-Switch: Results of ARP Protection ........ 211
ArubaOS-Switch: DHCP Snooping and ARP Protection ........ 212
ArubaOS-Switch: Guidelines for Using ARP Protection ........ 213
CLI Commands: Configuration of DHCP Snooping and ARP Protection ........ 214
Authenticate Routing Protocols ........ 215
Dynamic Routing Protocols ........ 215
Risks of Routing Protocol Manipulation ........ 215
Strategies for Securing Routing Protocols ........ 216
OSPF Authentication ........ 218
BGP MD5 Authentication ........ 220
CLI Commands: Configuration of Routing Protocol Authentication ........ 220
Summary ........ 221
Learning Check ........ 221

6 Network Authentication and Encryption Technologies ........ 223
Assumed Knowledge ........ 223
Overview ........ 223
Types of Network Authentication ........ 224
Why Network Authentication ........ 224
Layer 2 vs Layer 3 Authentication ........ 224
Captive Portal Authentication ........ 225
MAC-Auth ........ 226
802.1X Overview ........ 227
802.1X Roles ........ 228
802.1X Process: High-level Analogy ........ 229
802.1X Process: Communication Protocols ........ 231
802.1X Process: EAP Framework ........ 232
Examples of EAP Methods ........ 233
EAP-TLS Process ........ 235
Why EAP-TLS vs PEAP ........ 237
EAP-TLS Requirements ........ 239
EAP-TLS Configuration on Windows Client ........ 240

EAP-TLS on a Windows Domain Device .......... 243
Some Options for Deploying Certificates on User Devices .......... 244
WLAN Security .......... 245
Need for Secure Wireless Communications .......... 245
Overview of WLAN Security Options .......... 245
Overview of 802.11 Connection Steps .......... 247
WPA Key Hierarchy .......... 248
WPA Four-Way Handshake .......... 249
Krack: Attack on the Handshake .......... 250
Open WLANs .......... 250
Opportunistic Wireless Encryption (OWE) .......... 251
WPA/WPA2-Personal .......... 253
WPA/WPA2-Personal Issues .......... 253
WPA3-Personal .......... 254
WPA3-Personal Benefits .......... 255
Aruba mPSK .......... 255
WPA/WPA2-Enterprise .......... 256
WPA/WPA2-Enterprise Considerations .......... 257
WPA3-Enterprise .......... 258
Review of WPA3 + OWE Enhancements .......... 259
Additional Security with Management Frame Protection (MFP) .......... 260
Summary .......... 260
Learning Check .......... 261

**7 Enforce Edge Security with an Aruba Infrastructure .......... 263**
Assumed Knowledge .......... 263
Overview .......... 263
Scenario Introduction: First Steps in Protecting the Edge .......... 263
Enforce WPA3-Enterprise .......... 264
ArubaOS WPA3 Support .......... 264
How ArubaOS Wireless Devices Handle Users Associated to a WLAN .......... 265
Simple Example of Role Assignment .......... 266
Defining WLANs on MCs .......... 268
Attaching WLANs to APs .......... 269
Using the WLAN Wizard to Define WLANs .......... 270
Verifying the WLAN .......... 282
High-Level View of WPA-Enterprise Authentication to CPPM .......... 283
Additional Optional Tasks for the Authentication Server .......... 284
Adding RadSec to Secure RADIUS on Untrusted Links .......... 285

CLI Commands: MC Configuration for RadSec ................................286
Defining Multiple RADIUS/RadSec Servers in a Group ....................287
What Is Dynamic Authorization?....................................................287
Specifying a Dynamic Authorization RFC Server ............................288
Activating the Dynamic Authorization Server on WLANs .................290
Enforce Basic 802.1X on the Wired Network .......................................290
802.1X Configuration Process on Aruba Switches ...........................290
Specifying the RADIUS Server.......................................................291
Configuring RadSec on ArubaOS-Switches.....................................291
Supporting Multiple RADIUS Servers .............................................293
Ensuring Switches Support Dynamic Authorization ..........................294
CLI Commands: Aruba Switch CLI Configuration for RADIUS...........295
Enabling 802.1X ..........................................................................297
AOS-CX Port Access Roles...........................................................297
CLI Commands: Aruba Switch CLI Configuration for 802.1X ...........299
Summary.................................................................................300
Learning Check.........................................................................301

**8 Enforce Role-Based Authentication and Access Control...............303**
Assumed Knowledge ..................................................................303
Overview ..................................................................................303
Aruba Role-Based Firewall Policies ...............................................304
Scenario: Protecting the Edge with Role-Based Policies.....................304
ArubaOS Firewall versus a Traditional Firewall ...............................304
Role-Based ArubaOS Firewall.......................................................306
Review: What Is a Role? ...............................................................307
How ArubaOS Assigns a Client to a Role ......................................308
Example of Assigning Users to Different Roles with CPPM ................311
Aruba Role-Based Firewall Policies.................................................312
Components of a Role-Based Access Control Session Rule................313
Aliases.........................................................................................315
Benefits of Aliases ........................................................................316
Alias User ....................................................................................317
Session Rule Handling by Stateful ArubaOS Firewall .......................318
Application Layer Gateways (ALGs) ...............................................319
Bi-directional Rules and “user” versus “any”.....................................320
Translating Security Needs into Firewall Policies .............................321
Example Configuration.................................................................322
AppRF 2.0 ..................................................................................327
Example Creation of Application Rules ..........................................327

Application Rule Components in More Detail ....................................328
AppRF 2.0 Enforcement....................................................................329
PEF and WebCC Licenses ...............................................................330
Multi-Use Ports and Dynamic Segmentation.............................................330
The Goal of Multi-Use Ports ............................................................330
Aruba Switch Multi-Use Ports with Local Forwarding .........................332
Aruba Dynamic Segmentation: Tunneling to an MC...........................333
Use Cases for Tunneling Wired Traffic...............................................334
ArubaOS-Switch User Role Assignment ............................................334
AOS-CX Switch User Role Assignment..............................................335
Configuring Local Roles on Aruba Switches.......................................337
CLI Commands: Configuring User Roles on Aruba Switches.............................................................................339
Using Downloadable User Roles.......................................................340
CLI Commands: Enabling Downloading Roles on Aruba Switches ...............................................................................342
Setting up Tunneling Profile..............................................................344
Using Reserved VLAN .....................................................................346
CLI Commands: Configuring Tunneled-Node on Aruba Switches ...............................................................................347
CLI Commands: Configuring Jumbo Frames on Aruba Switches ...............................................................................348
Setting up the Aruba MC to Support the Tunnels...............................348
Viewing Tunnel Statuses...................................................................351
Viewing Tunneled Clients on Aruba Switches.....................................352
Viewing Tunneled Clients on an MC ................................................352
Summary.................................................................................................353
Learning Check........................................................................................353

9 **Identify and Classify Endpoints ..................................................357**
Assumed Knowledge...............................................................................357
Overview ................................................................................................357
Endpoint Classification Introduction .......................................................358
Scenario Introduction ......................................................................358
Better Device Visibility = Better Security............................................358
Overview of Endpoint Classification Methods....................................360
Aruba Solutions for Endpoint Classification.......................................361
Aruba ClearPass Policy Manager Device Profiler ....................................361
ClearPass Device Profiler within Policy Manager................................361
Overview of How ClearPass Profiles Devices ....................................363

Ongoing Classification and Detection of Conflicts ............................363
List of ClearPass Collectors............................................................364
DHCP Fingerprinting Overview ....................................................366
Common Options Used for DHCP Fingerprinting ............................366
Examples of Parameter List Options...............................................367
Example Dictionary Entry ............................................................369
Sending DHCP Fingerprinting Information with IP Helper Configuration .......................................................................370
HTTP User-Agent based Fingerprinting ..........................................371
How ClearPass Obtains HTTP User-Agent Strings ............................372
IF-MAP Profile Definition on ArubaOS...........................................373
Sending Device Fingerprinting Information to ClearPass with ArubaOS-Switches................................................................374
CLI Commands: Configuring Device Fingerprinting Policies on ArubaOS-Switches..................................................................377
Additional CPPM Methods............................................................377
Viewing Device Profiles in ClearPass ............................................382
Using Device Information to Control Endpoint Access (Example).......383
Aruba-No-DHCP-Fingerprint VSA.................................................384
Profiling and Connection Process..................................................385
Summary of Steps on ArubaOS Mobility Devices to Support ClearPass Device Profiler..................................................391
Summary of Steps on Aruba Switches to Support ClearPass Device Profiler ....................................................................393
CLI Commands: Commands on Aruba Switches to Support Device Profiling..........................................................................394
Aruba ClearPass Device Insight..........................................................395
ClearPass Device Insight...............................................................395
ClearPass Device Insight Architecture............................................396
Example Placements for ClearPass Device Insight Collectors .............397
Summary............................................................................................398
Learning Check ..................................................................................398

**10 Branch Security .......................................................................401**
Assumed Knowledge ..........................................................................401
Overview ...........................................................................................401
Introduction to Aruba SD-Branch Solutions ..........................................401
Key Branch Challenges.................................................................401
What Is SD-WAN?.......................................................................402
Why Aruba SD-Branch?...............................................................403

Aruba SD-Branch Solution Components ........................................ 405
Distributed Aruba Architecture ........................................ 406
Simplified SD-WAN with Aruba SD-Branch ........................................ 407
Simplified Onboarding and Lifecycle Management with Aruba SD-Branch ........................................ 408
Key Security Benefits in Aruba SD-Branch ........................................ 408
Role-based Access Segmentation ........................................ 409
Role-based Policies for LAN, Security, WAN ........................................ 410
BGW Trusted and Untrusted Interfaces ........................................ 411
How the BGW Learns Wireless Client Roles ........................................ 412
Dynamic Segmentation with Aruba Switches and BGWs ........................................ 413
Scalable Security Policies ........................................ 413
Orchestrated Cloud Security ........................................ 414
Summary ........................................ 415
Learning Check ........................................ 415

**11 Troubleshoot and Monitor ........................................ 417**
Assumed Knowledge ........................................ 417
Overview ........................................ 417
Logging and Monitoring ........................................ 418
Logging ........................................ 418
Logging Severity Levels ........................................ 418
Enabling Logs on Aruba MCs ........................................ 419
Enabling User-Debug and AP-Debug Logging ........................................ 420
Viewing Process Logs in the ArubaOS Web UI ........................................ 420
Viewing Logs on ArubaOS-Switches ........................................ 421
Viewing Logs on AOS-CX Switches ........................................ 422
Viewing Debug Information on Aruba Switches ........................................ 423
Defining Remote Logging Requirements ........................................ 424
Setting up Remote Logging on Aruba MCs ........................................ 425
Securing the MC Logs ........................................ 426
Setting up Secure Logging to a Syslog Server on Aruba Switches ........................................ 427
Controlling Which Event Logs Aruba Switches Forward ........................................ 428
Controlling Which Debugs Aruba Switches Forward ........................................ 429
CLI Commands: Configuring Logging on Aruba Switches ........................................ 430
Additional Traffic Monitoring through the ArubaOS Dashboard ........................................ 431
ArubaOS Client Table ........................................ 432
Using ArubaOS Traffic Analysis ........................................ 433
ArubaOS Traffic Analysis Dashboard ........................................ 434
ArubaOS Web UI versus Aruba AirWave ........................................ 435
Accessing Access Tracker in ClearPass Policy Manager (CPPM) ........................................ 435

Viewing Access Tracker Records....................................................436
Accessing Event Viewer in CPPM..................................................437
Aruba ClearPass Insight Dashboard and Inventory ..........................437
Aruba ClearPass Insight Reports...................................................438
Aruba ClearPass Insight Example Report .......................................439
Additional Aruba Monitoring Tools................................................439
Introduction to Troubleshooting Authentication Issues.............................440
Defining the Problem: Reproducing the Issue and Checking the Client .....................................................................440
Defining the Problem: Finding Commonalities.................................441
Collecting More Information .........................................................442
Determining Likely Issues .............................................................443
Applying and Evaluating Fixes......................................................444
Authentication Troubleshooting Scenarios............................................445
Scenario 1 ..................................................................................445
Scenario 2 ..................................................................................448
Scenario 3 ..................................................................................450
Packet Captures .....................................................................................452
Packet Capture and Traffic Mirroring.............................................452
Example Packet Capture/Analysis Application: Wireshark...............453
Reasons to Capture Packets .........................................................454
Where to Implement the Packet Capture ........................................454
Implementing a Packet Capture on an Aruba MC ...........................455
CLI Commands: Starting and Stopping Packet Captures on MCs........ 458
CLI Commands: Managing Packet Captures on MCs.......................458
Configuring Wireshark at Destination IP to Receive the Capture.........459
Implementing a Packet Capture on an Aruba AP ............................460
Implementing a Packet Capture for Traffic through an Aruba Switch.......................................................................460
Using Wireshark as the Destination for a Remote Packet Capture on ArubaOS-Switches .....................................................461
Summary...............................................................................................462
Learning Check .....................................................................................463

12 Implement Threat Detection and Forensics ................................465
Assumed Knowledge ..............................................................................465
Overview ..............................................................................................465
Forensics ...............................................................................................465
Digital Forensics ..........................................................................465
Chain of Custody..........................................................................466
Digital Chain of Custody ..............................................................467

Digital Forensics Steps....467
Forensic Policies....471
Analyze ArubaOS Wireless Intrusion Prevention (WIP) Events....472
Review Wireless Intrusion Prevention (WIP)....472
Review the Devices that Discover Threats....473
IDS/WIP Profile....476
ArubaOS Security Dashboard....477
Interpreting AP Classifications....478
Interpreting Client Classifications....479
Understanding the Risks Posed by Unauthorized Devices....480
Reviewing Some Ways to Mitigate Threats....482
Potential Follow up Actions....484
Understanding Unauthorized Device Policies....484
Viewing More Details about Interfering APs and Reclassifying Them....486
Viewing More Details about Rogue and Suspected Rogue APs....487
Analyzing the Match Type and Match Method....488
Understanding an ETH-GW-Wired-Mac-Table Match....488
Understanding Other Eth-Wired-MAC Matches....490
Other Match Types....491
Locating Detected Devices....491
Viewing Events and Logs....492
Additional WIP Features....494
Supplemental Reference Information on IDS Events....495
Review Licensing for WIP Features....501
Add Aruba AirWave for Compliance....501
Summary....502
Learning Check....502

13 Practice Exam....505
Introduction....505
Minimum Qualifications....505
Exam Details....505
Testing Objectives....505
Advice to Help You Take This Exam....506
Practice Exam Questions....507
Answers....519

Appendix A Glossary....................................................................529

Appendix B Learning Check Answers..............................................575
Chapter 1..........................................................................575
Chapter 2..........................................................................576
Chapter 3..........................................................................578
Chapter 4..........................................................................579
Chapter 5..........................................................................580
Chapter 6..........................................................................581
Chapter 7..........................................................................583
Chapter 8..........................................................................584
Chapter 9..........................................................................586
Chapter 10........................................................................587
Chapter 11........................................................................588
Chapter 12........................................................................590

Appendix C Supplemental Materials ................................................591
Chapter 2: Security Technologies..........................................591
Example TLS 1.2 Handshake..............................................591
Chapter 5: Secure LAN Protocols .........................................593
Supplemental Spanning Tree Information .......................593
Chapter 6: Network Authentication and Encryption Technologies............598
PEAP-MSCHAPv2 Process..................................................598
Chapter 9:.........................................................................601
DHCP Fingerprinting with ArubaOS Mobility Devices ......................601

Index.......................................................................................607

# 1 Security Threats and the Aruba Security Strategy

EXAM OBJECTIVES

✓ Describe common security threats, including malware, denial of service (DoS), spoofing, man-in-the-middle (MITM), and social engineering

✓ Identify the difference between a threat and a vulnerability

✓ Describe a kill chain and attack stages

## Assumed Knowledge

- Basics of IP networking
- Basics of Ethernet switching
- Basics of 802.11 wireless networks

## Overview

This chapter lays the groundwork for the rest of the study guide. In it you will learn about the threats to organizations' networks and the reasons why organizations require rigorous security more than ever before. You will then apply what you have learned in an activity.

Next you will learn about the specific stages of cyber attacks, from reconnaissance to extracting data onto the hacker's device.

Finally, you will learn why customers need to embrace a zero trust strategy for securing their network. You will examine the Aruba strategy for delivering a zero trust network and get an overview of the pieces of the strategy that this study guide will cover.

### Confidentiality, Integrity, and Availability (CIA)

Before you dive into an examination of threats against network services, take a moment to examine what these threats might compromise and what a secure network should deliver.

As defined by widespread industry models, a secure network should provide confidentiality, integrity, and availability (CIA). Confidentiality, sometimes called privacy, means that no one can read a message except the intended recipient. Integrity means that the message that the recipient receives matches the message that the actual transmitter originally sent. No one replaced the message with a different one or tampered with the message's contents. Integrity is related to authenticity, which means that the supposed transmitter of the message is the actual transmitter. These two pillars in the CIA model relate to the security of communications. The final pillar, availability, ensures that network services are available for legitimate users.

Throughout this chapter, you will look at threats to confidentiality, integrity, and availability. The rest of this study guide will explain how you can use an Aruba network infrastructure to fight those threats.

## Threat Overview

### Threats

You will begin by looking at common threats and the risks that they pose to your customers' networks and business.

A threat broadly refers to any action executed or initiated by a bad actor who uses or attempts to use the network inappropriately.

The results of threats include:

Data breaches, in which data is improperly exposed to those who are not authorized to use that data and want to use the data for their own purposes; for example, threats can expose users' credit card information or government-issued IDs.

Loss of network service; for example, threats can prevent legitimate users from reaching a company's web page.

### Vulnerabilities versus Threats

To properly secure your network from threats, you need to understand the relationship between threats and vulnerabilities, as shown in Figure 1-1.

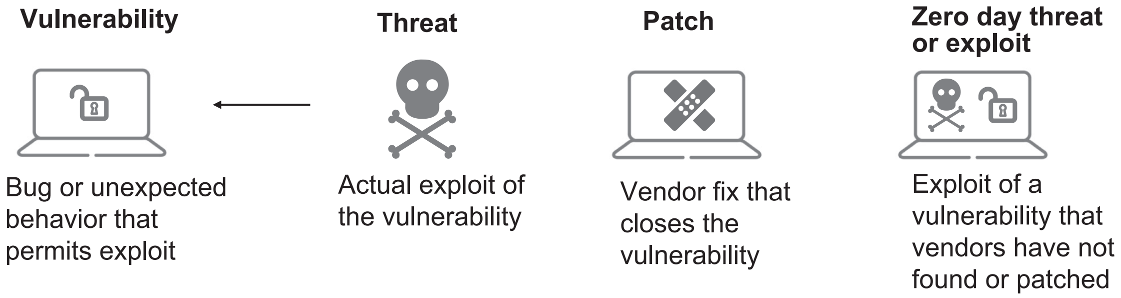
Vulnerability
Bug or unexpected behavior that permits exploit
Threat
Actual exploit of the vulnerability
Patch
Vendor fix that closes the vulnerability
Zero day threat or exploit
Exploit of a vulnerability that vendors have not found or patched

Figure 1-1: Vulnerabilities versus Threats

## Vulnerability

A vulnerability refers to a state in which a device or network is vulnerable to a threat. A vulnerability does not necessarily mean that an issue has occurred, but the risk of an exploit or attack is present. For example, a server operating system might have a bug that a hacker could exploit to cause the server to become unstable. Or perhaps software was coded in such a way that unintentionally allows hackers to gain privileged access without the proper credentials. Applications can also have vulnerabilities, as can the operating systems on network infrastructure devices.

## Patches

When security teams discover vulnerabilities, they inform the device, software, or OS vendor, which can then create a "patch" that closes the vulnerability. Vendors might push the patch to devices automatically—this is often what you are seeing when a window on your computer pops up, telling you that you need to restart your system to apply updates.

In a data center environment, security teams and server admins often work together to test those patches. After they have verified that the patches do not cause unintended changes to their servers' functionality, they deploy the patches. In a network environment, you also typically investigate and test software updates before deploying them in a production network.

## Zero-Day Vulnerabilities and Exploits

A zero-day vulnerability means that the vulnerability exists, but the vendor does not yet know about it.

A zero-day exploit means that unethical hackers have discovered the vulnerability and begun to exploit it before the vendor is aware of the vulnerability or before the vendor is able to create a patch. Because no patch yet exists for the vulnerability, many systems can be susceptible to the threat, making zero-day exploits highly dangerous.