

# HPE Network Security Expert Written Exam

## Exam description

This exam tests your ability to design, deploy, integrate, and articulate a PKI solution, allowing you to:

- Architect an enterprise-class network design aligned with security policies.
- Design role-based access control scheme using ClearPass/AOS/AOS-CX.
- Architect a solution that integrates ecosystem partners.
- Architect an enterprise-wide endpoint classification policy, design, and deploy proactive remediation.
- Use ClearPass Device Insight.

The certification exam and course were updated on October 15, 2024. See Release Notes.

## Ideal candidate for this exam

Typical candidates for this exam have 4–5 years of experience in networking with 2–3 years in security-focused fields.

Candidates are network architects responsible for auditing and/or remediating network vulnerabilities. They:

- Have experience designing and troubleshooting enterprise-level network solutions.
- Should articulate technical concepts associated with network security, e.g., RBAC, APT, endpoint classification, DOS, DDOS, policy enforcement, and unified SASE.
- Can compare and recommend HPE Aruba Networking security solutions.

## Exam contents

This exam has 70 questions.

## Advice to help you take this exam

- Updates to the certification exam and course went live on October 15, 2024. See Release Notes. This includes adding Axis Atmos Security Service Edge (SSE) Technology to the course and exam.
- Complete the training and review all course materials and documents before you take the exam.
- Exam items are based on expected knowledge acquired from job experience, an expected level of industry standard knowledge, or other prerequisites (events, supplemental materials, etc.).
- Successful completion of the course or study materials alone, does not ensure you will pass the exam.

## Objectives

This exam validates that you can:

Exam ID	HPE7-A10
Exam type	Proctored
Exam duration	2 hours 30 minutes
Exam length	70 questions
Passing score	66%
Delivery languages	English
Register for this Exam You need an HPE Learner ID and a Pearson VUE login and password.	
No reference material is allowed at the testing site. This exam may contain beta test items for experimental purposes.	
During the exam, you can make comments about the exam items. We welcome these comments as part of our continuous improvement process.	

Percentage of Exam	Sections/Objectives
58%	Protect and Defend 1.1 Explain and implement forensic techniques 1.2 Articulate how Aruba solutions help companies implement Zero Trust Security, including how these solutions integrate with a third-party ecosystem 1.3 Explain how Aruba solutions maps to local compliance 1.4 Define PKI best practices and implement certificate based authentication 1.5 Explain the role of device profiling and risk scoring in a company's security efforts 1.6 Explain and implement threat hunting techniques 1.7 Explain and implement role based access control 1.8 Design a detection strategy for rogue wireless devices and other wireless threats utilizing Aruba WIPS features 1.9 Implement Aruba Zero Trust Security with ClearPass Policy Manager (CPPM) and other ClearPass solutions 1.10 Design enterprise wide firewall policies (appRF, PEF, WIPS, WCC) for clients in a variety of wired and wireless architectures 1.12 Architect complex ACLs per wired interface and VLAN 1.13 Design and implement network analytic engine solutions for anomaly detection, correlation, auditing, and alerting 1.14 Explain how and why to integrate HPE Aruba Networking EdgeConnect and HPE Aruba Networking SSE solutions 1.15 Design and deploy secure client-to-site access using Aruba Central and Aruba gateways 1.16 Design and deploy Gateway IDS/IPS
38%	Analyze 2.1 Analyze logs, alerts and other features at expert level to detect threats 2.2 Remediate the security risk 2.3 Tune alerts 2.4 Design a workflow for Network Analytic Engine (NAE) script development 2.5 Implement endpoint classification and device profiling with CPDI (including profiling capabilities within Central Network Operations) 2.6 Integrate CPDI and CPPM and use device profiling data to tune policies and respond to vulnerabilities or threats
4%	Forensics 3.1 Perform a comprehensive threat analysis in a set timeframe 3.2 Package and deliver finding of comprehensive analysis

## For more information

Contact our program

© Copyright 2025 Hewlett Packard Enterprise. The information contained herein is subject to change without notice. The only warranties for HPE products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HPE shall not be liable for technical or editorial errors or omissions contained herein.

Information is as of October 2024, Revision 1