+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 10/08/2026

Sign Up

Aruba Network Security Fundamentals (ANSF) Training

4 days (28 hours)

Overview

HPE Aruba Networking offers technologies to protect wired and wireless networks. With hardened devices, secure LAN protocols, authentication and encryption mechanisms, and edge security, you'll have the foundation you need to build a network infrastructure that's better protected against threats.

Our Aruba Network Security Fundamentals (ANSF) training will help you build your knowledge to secure the infrastructures of your customers or partners. It is designed for network engineers and support technicians with six months to one year of experience in wired and wireless environments.

You'll learn to define security terminology, harden AOS-CX switches and AOS devices, and then apply appropriate protection mechanisms to LAN, WLAN, and WAN networks.

By the end of the course, you will be able to link threats to protective measures, select authentication and encryption technologies, and classify endpoints to tailor access controls.

This course also covers threat detection and the first steps in forensic analysis. Hands-on workshops will allow you to verify security measures and analyze logs in an investigative scenario.

Like all our training courses, this one will introduce you to **the latest stable version** of the technology and its new features.

Objectives

- Define security terminology
- Hardening AOS-CX and AOS devices
- Secure a WLAN and a wired LAN
- Secure the WAN
- Classify endpoints
- Detecting Threats and Investigating Through Forensic Analysis

Target Audience

- Network engineer in a client environment
- Network engineer in a partner environment
- Network support technician

Prerequisites

- Basic understanding of wired networking concepts, strongly recommended
- Basic understanding of wireless networking concepts, strongly recommended
- Basic understanding of security concepts, strongly recommended

Technical Prerequisites

- A computer equipped with a web browser and an SSH client for accessing lab equipment
- Stable Internet connection allowing the necessary access to the learning environment
- Access to the lab’s AOS-CX and AOS equipment according to the instructions provided prior to the training

Curriculum for our Aruba Network Security Fundamentals (ANSF) Training

[Day 1 - Morning]

Security Threats and Protection Strategies

- Security terminology: threat, vulnerability, risk, and attack
- Principles of confidentiality, integrity, and availability
- Common Threats in Wired and Wireless Environments
- Developing a protection strategy based on defense in depth and least privilege
- Hands-on Workshop: Analyzing a Business Scenario, Identifying Threats, and Matching Them with appropriate protective measures.

[Day 1 - Afternoon]

Network Security Technologies

- Functions of firewalls and access control lists
- Principles of network segmentation and traffic separation
- Roles of authentication, authorization, and audit mechanisms
- WAN Protection Through Filtering and Encrypted Tunnels
- The Role of Threat Detection and Logging in a Security Strategy
- Hands-on Workshop: Define a filtering policy for LAN and WAN traffic, then verify permitted and prohibited communications.

[Day 2 - Morning]

Hardening AOS-CX Switches

- Exposure surfaces of AOS-CX switches and hardening priorities
- Managing Administrator Accounts, Privileges, and Passwords
- Securing management access with SSH, HTTPS, and access restrictions
- Securing monitoring with SNMPv3 and log collection
- Reducing Exposed Services and Protecting Management and Control Paths
- Hands-on Workshop: Hardening an AOS-CX Switch and Verifying Administrative Access, Exposed Services, and Logged Events.

[Day 2 - Afternoon] Hardening

AOS Devices

- Identifying sensitive functions and management access on AOS devices
- Protecting administrator accounts and limiting privileges
- Restricting management access and reducing the attack surface
- Protecting control communications and administrative services
- Configuring logging to retain events useful for an investigation
- Hands-on Workshop: Applying a hardening procedure to an AOS device and verifying access controls and log reporting.

[Day 3 - Morning]

Secure LAN Protocols

- Risks Associated with Layer 2 Protocols in a Wired LAN
- Protection against unauthorized DHCP servers using DHCP snooping
- Protection against ARP spoofing with Dynamic ARP Inspection
- Protecting the topology with Spanning Tree security mechanisms
- Port Control and Coordination of Protections with LAN Segmentation
- Hands-on Workshop: Configure the security features available on the lab switch and verify their behavior in response to controlled DHCP, ARP, and Spanning Tree events.

[Day 3 - Afternoon]

Network Authentication and Encryption

- How 802.1X works and communication between the client, network equipment, and RADIUS server
- The role of EAP methods and certificates in network authentication
- Selecting WPA2 and WPA3 security mechanisms for a WLAN
- Applying authentication to wired and wireless LAN access
- Principles of IPsec VPN tunnels for protecting WAN communications
- Hands-on Workshop: Configure authenticated WLAN access, verify encryption, and analyze successful and failed authentication exchanges.

[Day 4 - Morning]

Edge security and endpoint classification

- Deploying security controls at the edge with HPE Aruba Networking
- Linking Identity, Role, and Network Access Rights
- Applying filtering policies to users and devices
- Principles of endpoint classification based on observed attributes
- Adapting access controls based on the endpoint’s profile and context
- Hands-on workshop: Classify multiple endpoints based on available information and verify the access rights associated with their profiles.

[Day 4 - Afternoon]

Threat detection and forensic analysis at the edge

- Identifying threat indicators in network and wireless events
- Interpreting alerts and distinguishing between expected events and suspicious activity
- Collecting and correlating logs, identities, and endpoint profiles
- Initial forensic analysis process and chronological reconstruction of events
- Preserving observed evidence and drawing investigative conclusions
- Hands-on workshop: Investigate a simulated incident using logs and alerts, identify the affected device, and reconstruct a well-documented timeline.

Target Audience

This training is intended for both individuals and companies—large or small—that wish to train their teams in new, advanced IT technologies or to acquire specific professional knowledge or modern methods.

Assessment at the Start of Training

The pre-training assessment complies with Qualiopi quality standards. Upon

final registration, the learner receives a self-assessment questionnaire that allows us to evaluate their estimated proficiency with various types of technologies, as well as their expectations and personal goals for the upcoming training, within the limits imposed by the selected format. This questionnaire also allows us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could pose challenges for monitoring and ensuring the smooth running of the training session.

Teaching Methods

Hands-On Training: 60% hands-on, 40% theory. Training materials distributed in digital format to all participants.

Organization

The course alternates between theoretical input from the instructor—supported by examples and reflection sessions—and group work.

Assessment

At the end of the session, a multiple-choice quiz is administered to verify that participants have successfully acquired the skills.

Certification

A certificate will be issued to each trainee who has completed the entire training program.

Training organization registered under number 11 75 54743 75. This registration does not constitute state accreditation.
© Ambient IT 2015-2026. All rights reserved. Paris, France - Switzerland - Belgium - Luxembourg