aruba a Hewlett Packard Enterprise company | AUTHORIZED TRAINING CENTER

fast lane

Implementing Aruba Network Security (AR-IANS)

Course Description

The Implementing Aruba Network Security course covers intermediate security concepts and prepares candidates to take the exam to achieve Aruba Certified Networking Security Professional (ACNSP) certification. This course helps admins use the Aruba portfolio to implement Zero Trust Security (ZTS) and protect their networks from threats. It explains how to configure Aruba network infrastructure and ClearPass solutions to authenticate and control both wired and wireless users, as well as remote users on a client-to-site VPN.

The course further explains how to collect a variety of contextual information on ClearPass Policy Manager (CPPM) and implement advanced role mapping and enforcement policies.

The course also covers using ClearPass Device Insight to enhance visibility. Learners will learn how to set up features such as the ArubaOSCX Network Analytics Engine (NAE), Aruba Wireless Intrusion Detection System/Intrusion Prevention System (WIDS/WIPS), and Aruba gateway IDS/IPS, as well as how to investigate alerts

Course Duration:

5 days

Prerequisites:

Aruba recommends that the candidate has attended the Aruba Network Security Fundamentals course prior to attending this professional level course. Or have equivalent experience and knowledge of network security fundamentals.

Objectives:

After you successfully complete this course, expect to be able to:

1- Protect and Defend

- Define security terminologies
  - PKI
  - Zero Trust Security
  - WIPS & WIDS
- Harden devices
  - Securing network infrastructure
  - Securing L2 & L3 protocols
- Secure a WLAN
  - Deploy AAA with CPPM
- Secure a wired LAN
  - Deploy AAA with CPPM
  - Deploy 802.1x
  - Deploy certificate based authentication for users & devices

- Secure the WAN
    - Understand Aruba's SD-Branch for automating VPN deployment
    - Design and deploy VPN with Aruba's VIA client
- Classify endpoints
    - Deploy endpoint classification to devices
- Implementing Aruba Network Security
    - Integrate ClearPass and CPDI

2- Analyze

- Threat detection
    - Investigate Central alerts
    - Interpret packet captures Evaluate endpoint postures
- Troubleshooting
    - Deploy and analyze results from NAE scripts
- Endpoint classification
    - Analyze endpoint classification data to identify risks
    - Analyze endpoint classification data on CPDI

3- Investigate

- Forensics
    - Explain CPDI capabilities of showing network conversations on supported
    - Aruba devices

Course Outline:

Aruba Security Strategy & ClearPass Fundamentals

- Explain Aruba Zero Trust Security
- Explain how Aruba solutions apply to different security vectors

Deploy Trusted Certificates to Aruba Solutions

- Describe PKI dependencies
- Set up appropriate certificates & trusted root CAs on CPPM

Implement Certificate - Based 802.1x

- Deploy AAA for WLANs with ClearPass Policy Manager (CPPM)
- Deploy certificate based authentication for users and devices

Implement Advanced Policies one the Role-Based ArubaOS Firewall

- Deploy AAA for WLANs with ClearPass Policy Manager (CPPM)
- Define and apply advanced firewall policies

Evaluate Endpoint Posture

- Evaluate different endpoint postures

Implement a Trusted Network Infrastructure

- Set up secure authentication and authorization of network infrastructure managers, including,
    - Advanced TACACS+ authorization
    - Multi-factor authentication
- Secure L2 and L3 protocols, as well as other protocols such as SFTP

Implement 802.1X and Role-Based Access Control on AOS- CX

- Deploy AAA for wired devices using ClearPass Policy Manager (CPPM), including local and downloadable roles
- Explain Dynamic Segmentation, including its benefits and use cases
- Deploy Dynamic Segmentation using VLAN steering
- Configure 802.1X authentication for APs

Implement Dynamic Segmentation on AOS-CX Switches

- Explain Dynamic Segmentation, including its benefits and use cases
- Deploy Dynamic Segmentation, including:
    - User-based tunneling (UBT)
    - Virtual network-based tunneling (VNBT)

Monitor with Network Analytics Engine (NAE)

- Deploy and use Network Analytics
- Engine (NAE) agents for monitoring

Implement WIDS/ WIPS

- Explain the Aruba WIPS and WIDS technology
- Configure AP rogue detection and mitigation

Use CPPM and Third-Party Integration to Mitigate Threats

- Describe log types and levels and use the CPPM Ingress Event Engine to integrate with third-party logging solutions
- Set up integration between the Aruba infrastructure and CPPM, allowing CPPM

Implement Device Profiling with CPPM

- Explain benefits and methods of endpoint classification on CPPM, including active and passive methods
- Deploy and apply endpoint classification to devices
- Analyze endpoint classification data on CPPM to identify risks

Introduction to ClearPass Device Insight

- Define ClearPass Device Insight (CPDI)
- Analyze endpoint classification data on CPDI

Deploy ClearPass Device Insight Define and deploy

- ClearPass Device Insight (CPDI)
- Analyze endpoint classification data on CPDI

Integrate CPDI with CPPM

- Integrate ClearPass Policy Manager (CPPM) and ClearPass Device Insight (CPDI)
- Mitigate threats by using CPDI to identify traffic flows and apply tags and CPPM to take actions based on tags

Use Packet Captures To Investigate Security Issues

- Perform packet capture on Aruba infrastructure locally and using Central
- Interpret packet captures

Establish a Secure Remote Access

- Explain VPN concepts
- Understand that Aruba SD-WAN solutions automate VPN deployment for the WAN
- Describe the Aruba 9x00 Series Gateways
- Design and deploy remote VPNs using Aruba VIA

Configure Aruba Gateway IDS/ IPS

- Describe the Aruba 9x00 Series Gateways
- Define and apply UTM policies

Use Central Alerts to Investigate Security Issues

- Investigate Central alerts
- Recommend action based on the analysis of Central alerts

Who Should Attend

Network engineer responsible for implementing security controls on enterprise networks.

Candidate can describe the network security stack (firewall, proxy, remote access, IDS/IPS, access control, NTA, UEBA)