Enterprise Computing Solutions - Education Services

TRAINING OFFERING

Du kan nå oss här

Kronborgsgränd 7, 164 46 Kista

Email: edu.ecs.se@arrow.com
Phone: +46 8 555 188 00

Implementing Aruba Network Security

CODE:	LENGTH:	PRICE:
ARU_INSF	40 Hours (5 days)	kr35,000.00

Description

The *Implementing Aruba Network Security* (IANS) 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 ArubaOS-CX 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 s.

- 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

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.

Session Dates

På begäran, kontakta oss

Ytterligare information

Denna utbildning finns också som utbildning på plats. Kontakta oss för mer information.