Network security challenges have evolved significantly over the years as users have become increasingly decentralized and attacks have become more sophisticated and persistent. The need for modern security technologies and best practices is critical to protect organization’s IT infrastructure from these new threats. Aruba's network security products provide 360⁰ of analytics-driven visibility, detection, control, and response to secure the enterprise.

The new Network Security certification from Aruba aims to enhance IT professionals ability to address current and future network security challenges. The Network Security Fundamentals course gives students a broad understanding of common security threats and vulnerabilities with an overview of important security technologies. The ACNSA validates skills with Aruba’s holistic security strategies including network policy enforcement with ClearPass, secure infrastructure capabilities embedded in Wi-Fi access points, switches, and controllers, and AI-powered continuous monitoring and attack detection software.

INTRODUCING ARUBA CERTIFIED NETWORK SECURITY ASSOCIATE (ACNSA)

An ACNSA certification validates your skills

To describe common security threats and vulnerabilities with an understanding of important security technologies.

✓ Protect and Defend
  ✓ Define security terminology
  ✓ Classify endpoints
  ✓ Secure a wired LAN

✓ Analyze
  ✓ Threat detection
  ✓ Troubleshooting
  ✓ Endpoint classification

✓ Investigate
  ✓ Forensics

✓ Harden devices
✓ Secure the WAN
✓ Secure a WLAN

An ACCA certification validates your skills

To contribute to the design and implementation of authentication and policy enforcement using the ClearPass product line.

✓ Understand services, enforcement policies and profiles
✓ Understand how to integrate and use Windows Active Directory in ClearPass
✓ Understand and can configure ClearPass guest
✓ Understand and can configure posture and profiling
✓ Understand and can configure device onboarding

www.arubanetworks.com

© Copyright 2020 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise 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. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.