Implementing Network Security

Category: Networking & Security | **Vendor:** HPE Aruba Networking

Duration: 40.00 hours (5 days) **32.5 CPD Hours** **Rating:** ⭐ 4.6 (5,878 reviews)

Course Information

Delivery Format: Instructor Led - Online

Course Overview

This course covers intermediate security concepts and prepares you for the ACP - Network Security (ACP-NS) certification exam. This training will help administrators use the HPE Aruba Networking portfolio to implement a Zero Trust Security (ZTS) protection model for their networks. Attending the course will teach you how to:

- Configure HPE Aruba Networking infrastructure with ClearPass solutions to authenticate/control both wired & wireless users, as well as remote users through Security Service Edge (SSE).
- Collect contextual information with ClearPass Policy Manager (CPPM) & implement advanced role mapping as well as enforcement policies.
- Use ClearPass Device Insight to enhance visibility.
- Set up features such as the AOS-CX Network Analytics Engine (NAE), HPE Aruba Networking Wireless IDS/IPS (WIDS/WIPS), & gateway IDS/IPS.
- Investigate alerts.

About This Course

- HPE Aruba Networking Security Strategy and ClearPass Fundamentals
- Deploy Trusted Certificates
- Implement Certificate-Based 802.1X
- Implement Advanced Policies on the Role-Based AOS Firewall
- Evaluate Endpoint Posture
- Implement a Trusted Network Infrastructure
- Implement 802.1X and Role-Based Access Control on AOS-CX
- Implement Dynamic Segmentation on AOS-CX Switches
- Monitor with Network Analytics Engine (NAE)
- Implement WIDS/WIPS
- Use CPPM and Third-Party Integration to Mitigate Threats
- Implement Device Profiling with CPPM
- Device Profiling with HPE Aruba Networking
- Deploy ClearPass Device Insight
- Integrate Device Insight with CPPM
- Use Packet Captures To Investigate Security Issues
- Secure Remote and Branch Access
- Configure HPE Aruba Networking Gateway IDS/IPS
- Use HPE Aruba Networking Central Alerts

Who Should Attend

Typical candidates for this course are network engineers responsible for implementing security controls on enterprise networks. Learners can describe the network security stack (firewall, proxy, remote access, IDS/IPS, access control, NTA, UEBA).

Prerequisites & Entry Requirements

General Prerequisites:

The following knowledge is recommended for this seminar:

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

Learning Outcomes

Upon successful completion of this course, participants will be able to:

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
- 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

Detailed Course Outline

- HPE Aruba Networking Security Strategy and ClearPass Fundamentals
- Deploy Trusted Certificates
- Implement Certificate-Based 802.1X
- Implement Advanced Policies on the Role-Based AOS Firewall
- Evaluate Endpoint Posture
- Implement a Trusted Network Infrastructure
- Implement 802.1X and Role-Based Access Control on AOS-CX
- Implement Dynamic Segmentation on AOS-CX Switches
- Monitor with Network Analytics Engine (NAE)
- Implement WIDS/WIPS
- Use CPPM and Third-Party Integration to Mitigate Threats
- Implement Device Profiling with CPPM
- Device Profiling with HPE Aruba Networking
- Deploy ClearPass Device Insight
- Integrate Device Insight with CPPM
- Use Packet Captures To Investigate Security Issues
- Secure Remote and Branch Access
- Configure HPE Aruba Networking Gateway IDS/IPS
- Use HPE Aruba Networking Central Alerts

Skills You Will Learn:

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
- 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

Frequently Asked Questions

Q: What delivery options are available for Implementing Network Security?

We offer multiple delivery formats:

- Live Instructor-Led Classroom Online (Virtual/Live Online)
- Traditional Instructor-Led Classroom Training (ILT)
- On-site delivery at your offices anywhere in United Kingdom
- Private dedicated courses customized for your team

Q: How many CPD hours does this course provide?

The 5-day Implementing Network Security course provides up to 32.5 CPD hours of structured learning. CPD certificates can be provided upon request.

Q: What is the duration of the Implementing Network Security training?

The training takes place over 5 day(s), with each day lasting approximately 40.00 hours including breaks for lunch and refreshments.

Q: Do you provide corporate training for Implementing Network Security?

Yes, we provide corporate training, dedicated training, and closed classes for Implementing Network Security. Training can take place anywhere in United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online allowing teams from across United Kingdom or internationally to attend.

Q: What related terms do people search for?

Popular related searches include: Implementing Network Security, Aruba Security, IANS

Q: Why choose Nexus Human for Implementing Network Security?

Nexus Human is recognized as one of the leading training providers. Our trainers have won multiple awards including:

- Small Firms Best Trainer Award
- National Training Partner of the Year (Ireland) - Multiple Years
- Global Top 30 Instructor Awards (2012, 2019, 2021)
- Tech Excellence Award Nominations
- Learning Performance Institute (LPI) External Training Provider Sponsor 2024

Q: Are there any discount codes available?

Yes! Use discount code **PENPAL5** when booking your Implementing Network Security training. Please note that only one discount code can be used per booking and cannot be combined with other special offers.

Nexus Human

Professional Training & Development

Email: info@nexushuman.com

Website: www.nexushuman.com

Phone: +353 1 XXX XXXX (Ireland) | +44 20 XXXX XXXX (UK)