



Enterprise Computing Solutions - Education Services

TRAINING OFFERING

You can reach us at:

Arrow Enterprise Computing Solutions Ltd, Part 1st Floor, Suite 1D/1, Central House, Otley Road, Harrogate, HG3 1UG

Email: educationteam.ecs.uk@arrow.com
Phone: 0870 251 1000

CODE:	LENGTH:	PRICE:
VMW_NSXIS4	40 Hours (5 days)	£3,230.00

Description

This five-day, hands-on training course provides you with the knowledge, skills, and tools to achieve competency in configuring, operating, and troubleshooting VMware NSX® for intrinsic security. This course introduces all the security features in NSX, including Distributed Firewall and Gateway Firewall, Intrusion Detection and Prevention (IDS/IPS), NSX Application Platform, NSX Malware Prevention, VMware NSX® Intelligence™, and VMware NSX® NDR™.

In addition, this course presents common configuration issues and gives a methodology to resolve them.

Objectives

By the end of the course, you should be able to meet the following objectives:

- Define the concepts related to information security
- Explain the different types of firewalls and their use cases
- Describe the operation of intrusion detection and intrusion prevention systems
- Differentiate between Malware Prevention approaches
- Describe the VMware intrinsic security portfolio
- Use NSX segmentation to implement Zero-Trust Security
- Configure user and role management
- Configure and troubleshoot Distributed Firewall, Identity Firewall, and time-based policies
- Configure and troubleshoot Gateway Security
- Use VMware Aria Operations™ for Logs and VMware Aria Operations™ for Networks to operate NSX firewalls
- Explain the security best practices related to grouping, tagging, and rule configuration
- Describe north-south and east-west service insertion
- Describe endpoint protection
- Configure and troubleshoot IDS/IPS
- Deploy NSX Application Platform
- Configure and troubleshoot NSX Malware Prevention
- Describe the capabilities of NSX Intelligence and NSX NDR

Audience

Experienced Security Administrators

Prerequisites

You should also have the following: Good understanding of TCP/IP services and protocols
Knowledge of and working experience with VMware vSphere® environments

Knowledge and working experience of network security, including:

- L2 through L7 firewalling
- Intrusion detection and prevention systems
- Malware prevention systems

The VMware Certified Technical Associate - Network Virtualization is recommended.

Programme

- 1 Course Introduction**
 - Introduction and course logistics
 - Course objectives
- 2 Security Basics**
 - Define the concepts related to information security
 - Explain the different types of firewalls and their use cases
 - Describe the operation of IDS/IPS
 - Differentiate between Malware Prevention approaches
- 3 VMware Intrinsic Security**
 - Define the VMware intrinsic security strategy
 - Describe the VMware intrinsic security portfolio
 - Explain how NSX aligns with the intrinsic security strategy
- 4 Implementing Zero-Trust Security**
 - Define Zero-Trust Security
 - Describe the five pillars of a Zero-Trust architecture
 - Define NSX segmentation and its use cases
 - Describe the steps needed to enforce Zero-Trust with NSX segmentation
- 5 User and Role Management**
 - Integrate NSX and VMware Identity Manager™
 - Integrate NSX and LDAP
 - Describe the native users and roles in NSX
 - Create and assign custom user roles
 - Explain object-based RBAC in a multitenancy environment
- 6 Distributed Firewall**
 - Configure Distributed Firewall rules and policies
 - Describe the NSX Distributed Firewall architecture
 - Troubleshoot common problems related to NSX Distributed Firewall
 - Configure time-based policies
 - Configure Identity Firewall rules
 - Configure the distributed firewall to block malicious IPs
- 7 Gateway Security**
 - Configure Gateway Firewall rules and policies
 - Describe the architecture of the Gateway Firewall
 - Identify and troubleshoot common Gateway Firewall issues
 - Configure TLS Inspection to decrypt traffic for both internal and external services
 - Configure URL filtering and identify common configuration issues
- 8 Operating Internal Firewalls**
 - Use VMware Aria Operations for Logs and VMware Aria Operations for Networks to operate NSX firewalls
 - Explain security best practices related to grouping, tagging, and rule configuration
- 9 Network Introspection**
 - Explain network introspection
 - Describe the architecture and workflows of north-south and east-west service insertion
 - Troubleshoot north-south and east-west service insertion
- 10 Endpoint Protection**
 - Explain endpoint protection
 - Describe the architecture and workflows of endpoint protection
 - Troubleshoot endpoint protection
- 11 Intrusion Detection and Prevention**
 - Describe the MITRE ATT&CK framework
 - Explain the different phases of a cyber attack
 - Describe how NSX security solutions can be used to protect against cyber attacks
 - Configure and troubleshoot Distributed IDS/IPS
 - Configure and troubleshoot North-South IDS/IPS
- 12 NSX Application Platform**
 - Describe NSX Application Platform and its use cases
 - Identify the topologies supported for the deployment of NSX Application Platform
 - Deploy NSX Application Platform
 - Explain the NSX Application Platform architecture and services
 - Validate the NSX Application Platform deployment and troubleshoot common issues
- 13 NSX Malware Prevention**
 - Identify use cases for NSX Malware Prevention
 - Identify the components in the NSX Malware Prevention architecture
 - Describe the NSX Malware Prevention packet flows for known and unknown files
 - Configure NSX Malware Prevention for east-west and north-south traffic

14 NSX Intelligence and NSX NDR

- Describe NSX Intelligence and its use cases
- Explain NSX Intelligence visualization, recommendation, and network traffic analysis capabilities
- Describe NSX NDR and its use cases
- Explain the architecture of NSX NDR in NSX
- Describe the visualization capabilities of NSX NDR

Session Dates

On request. Please [Contact Us](#)

Additional Information

[This training is also available as onsite training. Please contact us to find out more.](#)