Hewlett Packard
Enterprise

Course data sheet

VMware NSX for Intrinsic Security [V4.x] HT2S3S

HPE course number	HT2S3S
Course length	5 days
Delivery mode	ILT/VILT
View schedule, local pricing, and register	**View now**
View related courses	**View now**

This hands-on training course provides 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.

Why HPE Education Services?

- Comprehensive worldwide HPE technical, IT industry and personal development training
- Training and certification preparation for ITIL®, Security, VMware®, Linux, Microsoft and more
- Innovative training options that match individual learning styles
- Anytime, anywhere remote learning via HPE Digital Learner subscriptions
- Verifiable digital badges for proof of training, skill recognition and career development
- Simplified purchase options with HPE Training Credits

Audience

Experienced security administrators.

Prerequisites

Before Course participants should have:

- Good understanding of TCP/IP services and protocols
- Knowledge of, and working experience with, network security, including L2 through L7 firewalling, intrusion detection and prevention systems, malware prevention systems
- Knowledge of and working experience with VMware vSphere® environments.

The VMware Certified Technical Associate - Network Virtualization is recommended.

Course objectives

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

- Define concepts related to information security
- Explain 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 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 capabilities of NSX Intelligence and NSX NDR

Detailed course outline

1 Course Introduction	• Introductions and course logistics	• Course objectives
2 Security Basics	• Define concepts related to information security • Explain different types of firewalls and their use cases	• Describe 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 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 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 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 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 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 architecture and workflows of endpoint protection	• Troubleshoot endpoint protection
11 Intrusion Detection and Prevention	• Describe the MITRE ATT&CK framework • Explain 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 topologies supported for the deployment of NSX Application Platform • Deploy NSX Application Platform	• Explain NSX Application Platform architecture and services • Validate NSX Application Platform deployment and troubleshoot common issues

13 NSX Malware Prevention	• Identify use cases for NSX Malware Prevention • Identify components in the NSX Malware Prevention architecture	• Describe 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 visualization capabilities of NSX NDR

Learn more at

hpe.com/ww/learnvmware

Follow us:

Hewlett Packard
Enterprise

HT2S3S B.00, May 2023