# VMware NSX for Intrinsic Security [V4.x] (NSXIS4)

**ID** NSXIS4 **Price** 3,440.— €(excl. tax) **Duration** 5 days

This Advanced course is delivered directly by VMware.

## Course Overview

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.

Product Alignment

- VMware NSX 4.1.0

## Who should attend

Experienced security administrators

## This course is part of the following Certifications

VMware Certified Professional – Network Virtualization 2024 (VCP-NV 2024)

## Prerequisites

You should also have the following understanding or knowledge:

- Good understanding of TCP/IP services and protocols
- Knowledge and working experience of 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 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

## Course Content

- Course Introduction
- Security Basics
- VMware Intrinsic Security
- Implementing Zero-Trust Security
- User and Role Management
- Distributed Firewall
- Gateway Security
- Operating Internal Firewalls
- Network Introspection
- Endpoint Protection
- Intrusion Detection and Prevention
- NSX Application Platform
- NSX Malware Prevention

- NSX Intelligence and NSX NDR

## Detailed Course Outline

### Course Introduction

- Introduction and course logistics
- Course objectives

### 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

### VMware Intrinsic Security

- Define the VMware intrinsic security strategy
- Describe the VMware intrinsic security portfolio
- Explain how NSX aligns with the intrinsic security strategy

### 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

### 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

### 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

### 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

### 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

### 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

### Endpoint Protection

- Explain endpoint protection
- Describe the architecture and workflows of endpoint protection
- Troubleshoot endpoint protection

### 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

### 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

### 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

## 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

# About Fast Lane

Fast Lane is a global, award-winning specialist in technology and business training as well as consulting services for digital transformation. As the only global partner of the three cloud hyperscalers- Microsoft, AWS and Google- and partner of 30 other leading IT vendors, Fast Lane offers qualification solutions and professional services that can be scaled as needed. More than 4,000 experienced Fast Lane professionals train and advise customers in organizations of all sizes in 90 countries worldwide in the areas of cloud, artificial intelligence, cyber security, software development, wireless and mobility, modern workplace, as well as management and leadership skills, IT and project management.

## Fast Lane Services

- ✓ High End Technology Training
- ✓ Business & Soft Skill Training
- ✓ Consulting Services
- ✓ Managed Training Services
- ✓ Digital Learning Solutions
- ✓ Content Development
- ✓ Remote Labs
- ✓ Talent Programs
- ✓ Event Management Services

## Training Methods

- ✓ Classroom Training
- ✓ Instructor-Led Online Training
- ✓ FLEX Classroom – Classroom & Online Hybrid
- ✓ Onsite & Customized Training
- ✓ E-Learning
- ✓ Blended & Hybrid Learning
- ✓ Mobile Learning

## Technologies & Solutions

- ✓ Digital Transformation
- ✓ Artificial Intelligence
- ✓ Cloud
- ✓ Networking
- ✓ Cyber Security
- ✓ Wireless & Mobility
- ✓ Modern Workplace
- ✓ Data Center

**Worldwide Presence**
with high-end training centers around the globe

**Multiple Awards**
from vendors such as AWS, Microsoft, Cisco, Google, NetApp, VMware

**Experienced SMEs**
with over 19.000 combined certifications


**Germany**
**Fast Lane Institute for Knowledge Transfer GmbH**
Tel. +49 40 25334610
info@flane.de / www.flane.de

**Austria**
**ITLS GmbH**
(Partner of Fast Lane)
Tel. +43 1 6000 8800
info@itls.at / www.itls.at

**Switzerland**
**Fast Lane Institute for Knowledge Transfer (Switzerland) AG**
Tel. +41 44 8325080
info@flane.ch / www.flane.ch