

VMware NSX-T Data Center for Intrinsic Security

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-T™ Data Center for intrinsic security. In this course, you are introduced to all the security features in NSX-T Data Center, including Distributed Firewall and Gateway Firewall, Intrusion Detection and Prevention (IDS/IPS), NSX Application Platform, NSX Malware Prevention, VMware NSX® Intelligence™, and VMware NSX® Network Detection and Response™.

In addition, you are presented with common configuration issues and given a methodology to resolve them.

Course Objectives

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

- Define information-security-related concepts
- 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
- Implement Zero-Trust Security using VMware NSX® segmentation
- Configure user and role management
- Configure and troubleshoot Distributed Firewall, Identity Firewall, and time-based policies
- Configure and troubleshoot Gateway Security
- Use VMware vRealize® Log Insight™ for NSX™ and VMware vRealize® Network Insight™ 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 Network Detection and Response

Target Audience

- Experienced security administrators

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 and KVM-based environments

The VMware Certified Technical Associate - Network Virtualization is recommended.

Course Delivery Options

- Classroom
- Live Online
- [Private Training](#)

Product Alignment

- VMware NSX-T Data Center 3.2.x

Course Modules

1 Course Introduction

- Introductions and course logistics
- Course objectives

2 Security Basics

- Define information-security-related concepts
- 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-T Data Center 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-T Data Center and VMware Identity Manager™
- Integrate NSX-T Data Center and LDAP
- Describe the native users and roles in NSX-T Data Center
- Create and assign custom user roles

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

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 vRealize Log Insight for NSX and vRealize Network Insight 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



VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

© 2022 VMware, Inc. All rights reserved. The product or workshop materials is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/download/patents.html>. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

VMware warrants that it will perform these workshop services in a reasonable manner using generally accepted industry standards and practices. THE EXPRESS WARRANTY SET FORTH IS IN LIEU OF ALL OTHER WARRANTIES, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE WITH RESPECT TO THE SERVICES AND DELIVERABLES PROVIDED BY VMWARE, OR AS TO THE RESULTS WHICH MAY BE OBTAINED THEREFROM. VMWARE WILL NOT BE LIABLE FOR ANY THIRD-PARTY SERVICES OR PRODUCTS IDENTIFIED OR REFERRED TO CUSTOMER. All materials provided in this workshop are copyrighted by VMware ("Workshop Materials"). VMware grants the customer of this workshop a license to use and make reasonable copies of any Workshop Materials strictly for the purpose of facilitating such company's internal understanding, utilization, and operation of its licensed VMware product(s). Except as set forth expressly in the sentence above, there is no transfer of any intellectual property rights or any other license granted under the terms of this workshop. If you are located in the United States, the VMware contracting entity for the service will be VMware, Inc., and if outside of the United States, the VMware contracting entity will be VMware International Limited.

- 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 Network Detection and Response

- Describe NSX Intelligence and its use cases
- Explain NSX Intelligence visualization, recommendation, and network traffic analysis capabilities
- Describe NSX Network Detection and Response and its use cases
- Explain the architecture of NSX Network Detection and Response in NSX-T Data Center
- Describe the visualization capabilities of NSX Network Detection and Response

Contact

If you have questions or need help registering for this course, click [here](#).



VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
© 2022 VMware, Inc. All rights reserved. The product or workshop materials is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/download/patents.html>. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

VMware warrants that it will perform these workshop services in a reasonable manner using generally accepted industry standards and practices. THE EXPRESS WARRANTY SET FORTH IS IN LIEU OF ALL OTHER WARRANTIES, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE WITH RESPECT TO THE SERVICES AND DELIVERABLES PROVIDED BY VMWARE, OR AS TO THE RESULTS WHICH MAY BE OBTAINED THEREFROM. VMWARE WILL NOT BE LIABLE FOR ANY THIRD-PARTY SERVICES OR PRODUCTS IDENTIFIED OR REFERRED TO CUSTOMER. All materials provided in this workshop are copyrighted by VMware ("Workshop Materials"). VMware grants the customer of this workshop a license to use and make reasonable copies of any Workshop Materials strictly for the purpose of facilitating such company's internal understanding, utilization, and operation of its licensed VMware product(s). Except as set forth expressly in the sentence above, there is no transfer of any intellectual property rights or any other license granted under the terms of this workshop. If you are located in the United States, the VMware contracting entity for the service will be VMware, Inc., and if outside of the United States, the VMware contracting entity will be VMware International Limited.