+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 02/05/2026

Register

NSX Security Training: Microsegmentation & Zero Trust

3 days (21 hours)

Overview

The NSX Security training course teaches you how to implement effective microsegmentation and a Zero Trust approach to reduce the attack surface and contain lateral movement. You will learn how to translate business requirements (third-party apps, PCI, multi-tenant environments) into operational security policies.
multi-tenant environments) into operational security policies.

You will build a segmentation strategy based on flow inventory, dynamic group definition, and the application of distributed rules as close as possible to workloads. The focus is on policy readability, exception reduction, and lifecycle management (change, audit, rollback).

The approach is practical: guided workshops, demos, troubleshooting exercises, and validation through connectivity tests. Deliverables include a flow matrix, a naming model, documented NSX rules, and a hardening and operation checklist.

Like all our training courses, this one will introduce you to **the latest stable version** of the technology and its new features.

Objectives

- Map application flows and define a microsegmentation strategy.
- Create dynamic groups and consistent security policies.
- Apply Zero Trust (deny by default, least privilege) to specific cases.
- Implement logging, traceability, and validation (logs, tests, audits).
- Troubleshoot connectivity issues related to rules and insertion services.

Target audience

- VMware virtualization administrators/engineers (vSphere/NSX)
- Network security/SOC engineers
- Infrastructure/private cloud architects
- Ops/DevOps responsible for multi-tier applications

Prerequisites

- Good networking fundamentals: TCP/IP, VLAN, routing, L3/L4 firewalls
- Security concepts: segmentation, ACL, Zero Trust principles
- Knowledge of vSphere: VM, vNIC, vSwitch/port groups
- Log reading and diagnostics (ping, traceroute, ports)

Technical prerequisites

- PC with 16 GB RAM (minimum 8 GB), 4-core CPU recommended
- Windows, macOS, or Linux with a modern browser
- Access to an NSX lab (provided by the organization) and VPN client if necessary
- Tools: terminal (PowerShell/Bash), text editor, SSH client

Our NSX Security training program: microsegmentation & Zero Trust

[Day 1 - Morning]

NSX Security fundamentals and Zero Trust approach

- Positioning NSX in the architecture (NSX Manager, Transport Nodes, segments, T0/T1)
- Zero Trust principles: least privilege, explicit verification, reduction of attack surface
- Key NSX security concepts: Distributed Firewall (DFW), groups, services, policies
- Microsegmentation models: by application, by environment (dev/test/prod), by trust zone
- Hands-on workshop: Getting started with the NSX interface and locating security objects (DFW, Groups,
  Services).

[Day 1 - Afternoon]

Microsegmentation with the Distributed Firewall (DFW)

- Understanding DFW L2/L3/L4 and the impact on east-west traffic
- Building dynamic groups (tags, naming, VM criteria) and avoiding IP-based rules
- Writing effective rules: sources/destinations, services, scope, log, default rule
- Best practices: policy structure, priorities, naming, change management

- Hands-on workshop: Create a DFW "deny by default" policy and allow only necessary application flows.

[Day 2 - Morning]

Discovering flows and progressive security

- Collecting and interpreting flows: DFW logs, visibility tools, identifying application dependencies
- "Observe > model > enforce" approach to limit service interruptions
- Failover strategies: monitoring, partial enforcement, temporary exceptions
- Service management: ports, protocols, service groups, and standardization
- Hands-on workshop: Establish a flow matrix (app tiers) and translate it into DFW rules.

[Day 2 - Afternoon]

Advanced policy administration and troubleshooting

- Policy organization: sections, third-party policies, global vs. application rules
- Traceability and auditing: logging, rule justification, exception management
- Troubleshooting: rule hit analysis, logs, group verification, rule conflict resolution
- Optimization: reducing the number of rules, reusing objects, performance and readability
- Hands-on workshop: Diagnosing a blocked flow and correcting the policy without excessively expanding access.

[Day 3 - Morning]

Zero Trust applied: segmentation by zones and access control

- Defining trust zones (users, apps, data, management) and their interconnection rules
- Model "default deny" policies with controlled exceptions
- Object identity management: tags, conventions, integration with the VM lifecycle
- Use case: isolation of a sensitive environment (bastion, management, backup)
- Hands-on workshop: Design a 3-zone segmentation (Front/App/DB) and apply the minimum necessary rules.

[Day 3 - Afternoon]

Industrialization, compliance, and preparation for operation

- Standardize: policy templates, service catalogs, "golden" rules
- Automate: Infrastructure as Code principles for objects and rules (API/internal tool approach)
- Operational controls: periodic reviews, rule cleanup, change management
- Security reporting: compliance evidence, indicators (active rules, exceptions, logs)
- Hands-on workshop: Produce a microsegmentation runbook and rule review checklist.

Target companies

This training is intended for both individuals and companies, large or small, wishing to train their teams in advanced new IT technology or to acquire specific business knowledge or modern methods.

Positioning at the start of training

The positioning at the start of the training complies with Qualiopi quality criteria. Upon final registration, the learner receives a self-assessment questionnaire that allows us to assess their estimated level of knowledge of different types of technologies, their expectations and personal objectives for the upcoming training, within the limits imposed by the selected format. This questionnaire also allows us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could be problematic for the monitoring and smooth running of the training session.

Teaching methods

Practical training: 60% practical, 40% theory. Training materials distributed in digital format to all participants.

Organization

The course alternates between theoretical input from the trainer, supported by examples and discussion sessions, and group work.

Assessment

At the end of the session, a multiple-choice questionnaire is used to verify that the skills have been correctly acquired.

Certification

A certificate will be issued to each trainee who has completed the entire training course.