MERCURY

Fortinet NSE 4: FortiOS Administrator Training Course

4 – 8 July 2027
Online



Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

Fortinet NSE 4: FortiOS Administrator Training Course

Ref: 46_1082660 **Date:** 4 – 8 July 2027 **Location:** Online **Fees:** 2900 Euro

The Fortinet NSE 4: FortiOS Administrator Training Course is a one-week course for network engineers, systems administrators, security analysts, and technical support specialists responsible for perimeter defense. Working with security profiles, routing policies, and virtual domains, you assemble a complete FortiOS Security and Infrastructure Dossier. Mercury Training Center delivers this course to help you configure, manage, and monitor enterprise network security across production environments.

About This Course

Misconfigured firewall policies, uninspected encrypted traffic, and uncoordinated routing failover expose enterprise networks to service interruptions and perimeter breaches. To follow this course, you must already understand fundamental IP routing, address translation, and basic network defense. Through hands-on administration workflows, you practice deploying firewall inspection engines, establishing encrypted tunnels, and configuring high-availability clusters.

Who It Is For

- Professionals responsible for configuring Next-Generation Firewall inspection policies and Network Address Translation rules
- Professionals responsible for deploying secure IPsec and SSL VPN tunnels for enterprise remote connectivity
- Professionals responsible for managing high-availability firewall clusters and SD-WAN routing topologies
- Professionals responsible for implementing user authentication and directory integration across enterprise network perimeters

This course is not for helpdesk technicians seeking entry-level computer support concepts, who are better served by foundational IT support coursework, nor is it for enterprise governance officers requiring high-level cyber policy overviews, who would gain more from foundational information risk management training.

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

Competencies You Will Build

- Security Profile Enforcement: Deploying web filtering, antivirus inspection, application control, and intrusion prevention engines to secure perimeter traffic.
- Encrypted Tunnel Architecture: Provisioning point-to-point IPsec tunnels and remote access SSL VPN interfaces to safeguard corporate data flows.
- Resilient Infrastructure Management: Configuring firewall clustering protocols and policy-based routing to ensure continuous network uptime.
- Identity and Access Integration: Synchronizing Fortinet Single Sign-On and directory services to enforce identity-aware access rules.
- Network Segmentation Control: Partitioning physical firewalls into Virtual Domains to isolate tenant environments and restrict lateral movement.

What You Will Be Able to Do

By the end of the course you will be able to:

- From enterprise security requirements, configure firewall policies with deep packet inspection to block unauthorized application traffic.
- Given remote branch topologies, establish redundant site-to-site IPsec VPN tunnels with automated failover mechanisms.
- Using active directory infrastructures, integrate Fortinet Single Sign-On agents to enforce identity-based perimeter security policies.
- From high-availability requirements, deploy FortiGate active-passive clusters with synchronized session states and automated heartbeats.
- Given multi-tenant network designs, configure Virtual Domains and inter-VDOM routing links to separate distinct operational environments.
- Using administrative event monitors, configure centralized logging and alerting profiles aligned with cybersecurity audit baselines.

Course Content

Day 1: FortiGate Deployment and Policy Configuration

- FortiOS System Architecture and Initial Management Interface Setup
- Next-Generation Firewall Policy Creation and Service Object Definition
- Source, Destination, and Port Address Translation Implementations
- Firewall Session Diagnostics and Flow-Based Inspection Modes
- Administrative Role-Based Access and Configuration Backup Procedures

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

Day 2: Threat Prevention and Identity Integration

- Antivirus and Sandboxing Inspection Profiles for Malware Defense
- Web Filtering Categories, Quotas, and SSL Inspection Topologies
- Application Control Engine Tuning and Cloud Service Discovery
- Intrusion Prevention System Signatures and Denial of Service Defense
- Fortinet Single Sign-On Integration with Enterprise Directory Services

Day 3: Routing Architectures and Virtual Domains

- Static Routing, Dynamic Protocols, and Equal-Cost Multi-Path Behaviors
- Policy-Based Routing and Application-Aware SD-WAN Implementation
- Virtual Domains Configuration for Multi-Tenant Infrastructure Separation
- Inter-VDOM Links and Controlled Traffic Segmentation Mechanisms
- VLAN Sub-Interfaces and Layer 2 Transparent Mode Topologies

Day 4: Secure Remote Access and High Availability

- Site-to-Site IPsec VPN Phase 1 and Phase 2 Tunnel Negotiation
- Redundant IPsec Topologies with Dead Peer Detection Protocols
- SSL VPN Portals, Tunnel Modes, and Client-Side Authentication Rules
- Active-Passive and Active-Active High Availability Cluster Setup
- Cluster Synchronization Parameters and Failover Monitoring Diagnostics

Day 5: Operational Diagnostics and Infrastructure Hardening

- Exercise on Multi-Tenant Virtual Domain Isolation and Inter-Routing
- Exercise on Fault-Tolerant High-Availability Failover and Session Recovery
- Exercise on Deep Packet SSL Inspection and Application Filtering Policies
- Exercise on Centralized Event Logging and Audit Trail Validation
- Final Assembly and Validation of the FortiOS Security and Infrastructure Dossier

Case Studies and Exercises

These suggested activities provide practical application of security administration methods across different operational environments:

- Case study: A commercial banking network where you configure strict application inspection, isolate banking applications within dedicated Virtual Domains, and verify encrypted branch connectivity.
- Case study: A regional hospital infrastructure where you implement role-based access for clinical workstations, establish secure SSL VPN remote portals, and enforce antivirus filtering on medical data transfers.
- Exercise: A manufacturing plant where you configure active-passive clustering, establish policy-based routing across redundant links, and resolve high-availability synchronization discrepancies.
- Exercise: A central enterprise headquarters where you deploy deep packet SSL inspection, build identity-based firewall rules, and validate perimeter event logging.

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

What You Take Back

The FortiOS Security and Infrastructure Dossier provides validated deployment checklists, policy architectures, and troubleshooting workflows to support network security administration immediately during your first month back at work. You will use it to standardize firewall deployments, troubleshoot routing failovers, and verify perimeter defense postures.

- Validated Next-Generation Firewall policy templates and inspection profile baselines
- IPsec and SSL VPN tunnel design architectures with preconfigured authentication flows
- High-availability cluster failover runbooks and synchronization validation checklists
- Virtual Domain partitioning matrices for secure multi-tenant network segmentation

Quick Answers FAQ

What background is required before attending the Fortinet NSE 4: FortiOS Administrator Training Course?

You need working familiarity with networking fundamentals, including TCP/IP addressing, subnetting, standard routing protocols, and firewall concepts. Practical experience in administering local area networks or configuring basic network appliances helps you execute the hands-on administration labs effectively.

How does this course differ from general enterprise network security training?

General enterprise network security training covers theoretical perimeter defense across diverse vendor architectures. This course focuses specifically on FortiOS administration, providing direct instruction in Next-Generation Firewall configuration, proprietary clustering protocols, Virtual Domain segmentation, and native threat prevention engines.

Why is deep SSL inspection critical when managing FortiOS firewall policies?

Most malicious web traffic and enterprise data leaks hide inside encrypted transport layers. Deep SSL inspection decrypts and analyzes secure traffic flows at the gateway, enabling FortiOS security engines to detect advanced malware, block restricted applications, and maintain network visibility.

What tangible materials do participants retain from the Fortinet NSE 4: FortiOS Administrator Training Course?

You retain the FortiOS Security and Infrastructure Dossier, which contains firewall policy configurations, high-availability deployment runbooks, VPN implementation guides, and network troubleshooting checklists for operational use in enterprise production environments.

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

For Your Manager

The team member will be able to administer enterprise perimeter defenses, deploy resilient VPN architectures, and configure high-availability FortiGate clusters across production environments. They return with the FortiOS Security and Infrastructure Dossier, which will be used immediately to audit existing firewall policies, harden perimeter segmentation, and resolve network connectivity issues.