CONCEPT

Fortinet NSE 4 and FCP Network Security Training Course



Fortinet NSE 4 and FCP Network Security Training Course

Introduction:

Fortinet NSE 4 and FCP Network Security Training is a one-week course for network security administrators, perimeter defence engineers, systems infrastructure specialists, and security operations analysts, culminating in a FortiGate Security and Infrastructure Deployment Dossier. Uncoordinated firewall policies, uninspected internal traffic, and inconsistent identity mappings create critical security exposures and operational disruptions across enterprise networks. Nominees already administer IP networks, configure static routing, and maintain standard access lists, advancing their operational capability through hands-on lab exercises. CoreConcept Training Center delivers this Fortinet NSE 4 and FCP Network Security Training to establish robust, defensible boundary security controls across enterprise architectures.

Course Objectives:

- Configure FortiOS firewall policies, security profiles, and network address translation to enforce positive security access controls.
- Implement Fortinet Single Sign-On and user-identity firewall rules to authenticate corporate users across enterprise segments.
- Deploy secure site-to-site IPsec tunnels and remote-access SSL VPNs to safeguard corporate communications across distributed environments.
- Establish FortiGate High Availability clusters and Virtual Domains to maintain service redundancy and secure multi-tenant network separation.
- Execute systematic diagnostics, firewall configuration reviews, and security logging routines to verify policy compliance and operational integrity.
- Assemble the FortiGate Security and Infrastructure Deployment Dossier to standardise perimeter security and internal network inspection.

Target Audience:

- Network security administrators responsible for managing firewall policies, implementing access controls, and maintaining perimeter gateway availability.
- Perimeter defence engineers responsible for deploying virtual private networks, configuring intrusion prevention, and securing network boundaries.
- Systems infrastructure specialists responsible for integrating directory services, establishing high-availability clusters, and configuring routing interfaces.
- Security operations analysts responsible for monitoring firewall traffic logs, inspecting threat events, and auditing security rule configurations.

Course Outline:

Day 1: Security Fabric Architecture and Initial Device Deployment

- FortiOS 7.2 Initial Setup Establishing Interface Addressing and Management Access
- FortiGate Administrative Profiles Configuring Role-Based Access Control and Authentication
- FortiOS Security Fabric Deploying Device Telemetry and Centralised Visibility
- FortiGate Transparent Mode Configuring Layer Two Packet Forwarding and Filtering
- Network Security Audit Procedures Reviewing Baseline Firewall Rule Configurations

Day 2: Firewall Policies, Authentication, and Identity Management

- FortiOS Next-Generation Firewall Defining Positive Security Whitelisting Rules
- Fortinet Single Sign-On Integrating Active Directory Domain User Identity Mappings
- FortiGate Central NAT Configuring Source and Destination Address Translations
- FortiOS Certificate Inspection Implementing Deep SSL Decryption and CA Validation
- FortiGate User Authentication Rules Binding Group Permissions to Network Policies

Day 3: Threat Inspection Profiles and Remote Access Protection

- FortiGate Antivirus Engine Deploying Flow-Based and Proxy-Based Malware Inspection
- FortiOS Web Filtering Profiles Enforcing URL Categorisation and Threat Blocking
- FortiGate Application Control Profiles Identifying and Restricting Application Layer Protocols
- FortiGate Intrusion Prevention System Tuning Signature Baselines and Protocol Anomaly Filters
- FortiGate SSL VPN Establishing Client-to-Gateway Tunnels and Multi-Factor Authentication

Day 4: Infrastructure Routing, Virtualisation, and High Availability

- FortiOS Static and Dynamic Routing Configuring OSPF and BGP Inter-VLAN Routing
- FortiGate Virtual Domains Partitioning Multi-Tenant Traffic and Administrative Boundaries
- FortiGate High Availability Deploying Active-Passive and Active-Active Heartbeat Clustering
- FortiGate IPsec VPN Configuring Redundant Site-to-Site Tunnels and Routing
- FortiGate Diagnostic CLI Commands Troubleshooting Kernel Packet Flow and Session Tables

Day 5: Enterprise Network Security Lab and Technical Synthesis

- FortiGate Lab Deploying Datacenter East-West Micro-Segmentation Controls
- FortiGate Lab Hardening Enterprise Perimeter Firewalls and VPN Tunnels
- FortiGate Lab Simulating Real-Time Threat Mitigation and Traffic Failover
- FortiGate Lab Conducting Six-Month Firewall Rule Lifecycle Reviews
- FortiGate Security and Infrastructure Deployment Dossier Completing Enterprise Implementation Records

Skills You Will Gain:

- Next-Generation Firewall Policy Administration
- Identity-Based Access Control Configuration
- Encrypted Traffic SSL Inspection
- Intrusion Prevention Signature Tuning
- Virtual Private Network Architecture
- High-Availability Cluster Implementation
- Virtual Domain Multi-Tenant Partitioning
- Firewall Configuration Security Auditing

Why Attend This Course:

- Deliver the FortiGate Security and Infrastructure Deployment Dossier to the chief information security officer to establish standardised perimeter controls.
- Select appropriate inspection modes, authentication profiles, and routing policies to balance network performance against security requirements.
- Eliminate unmonitored lateral movements, configuration drift, and uninspected encrypted traffic that lead to costly security breaches.
- Guide engineering colleagues in diagnosing kernel session flows, configuring high-availability failovers, and executing periodic firewall audits.

Conclusion:

Following this course, the organisation deploys the FortiGate Security and Infrastructure Deployment Dossier to standardise perimeter security and internal network segmentation across operating units. The head of IT infrastructure and the cybersecurity operations manager use this deliverable to approve firewall policy modifications, validate authentication integrations, and supervise high-availability configurations. Within six months of implementation, the network operations team should conduct a structured review of active firewall rules, failover logs, and security profile efficacy to eliminate dormant access paths and verify continuous adherence to internal architecture standards.

Frequently Asked Questions FAQ:

Which roles should an organisation nominate for the Fortinet NSE 4 and FCP Network Security Training?

Organisations should nominate network security administrators, perimeter defence engineers, network systems specialists, and security operations analysts. Nominees are operational practitioners responsible for maintaining firewall interfaces, implementing network access rules, managing secure remote connectivity, and monitoring infrastructure security events across enterprise environments.

What should nominees already do at work before attending the Fortinet NSE 4 and FCP Network Security Training?

Nominees should already manage enterprise IP networking, administer basic routing protocols, and operate standard network access lists. Familiarity with fundamental firewall concepts, domain name resolution, and basic operating system networking commands ensures nominees immediately engage with advanced security policies, inspection profiles, and high-availability clustering.

What does the organisation receive when the participant returns from the Fortinet NSE 4 and FCP Network Security Training?

The organisation receives a completed FortiGate Security and Infrastructure Deployment Dossier. This practical deliverable provides production-ready configuration templates, verified high-availability failover architectures, encrypted virtual private network specifications, and documented procedures for executing semi-annual firewall rule reviews across operational networks.

Which standard or framework does the Fortinet NSE 4 and FCP Network Security Training follow?

The course follows the Fortinet Certified Professional and Fortinet Network Security Expert curriculum for FortiOS. It incorporates comparative technical controls from applicable network security templates, including positive security whitelisting, layer-seven application filtering, user-identity enforcement, and mandatory six-month firewall configuration review workflows for critical systems.