BLACKBIRD FOR TRAINING

Advanced FortiGate Administrator Training Course



Advanced FortiGate Administrator Training Course

Introduction:

This FortiGate Administrator Training Course equips you to configure, operate, and secure enterprise perimeter firewalls using FortiOS across five intensive days. You will build an enterprise FortiGate Network Security Infrastructure and Policy Baseline covering high availability, policy change documentation, and threat inspection profiles. You need a foundational understanding of networking concepts, IP addressing, and core routing protocols to benefit from this practitioner-level course. You will practise through hands-on lab sessions, deploying firewall security policies, VPN tunnels, and threat prevention filters directly on active FortiGate instances.

Course Objectives:

- Configure FortiGate network interfaces and static routing within dual-stack operating environments.
- Build stateful firewall policies and address objects to enforce segmented perimeter boundaries.
- Deploy FortiOS security profiles including antivirus, intrusion prevention, web filtering, and application control.
- Implement route-based IPsec site-to-site tunnels and remote-access SSL VPN portals for authenticated enterprise users.
- Configure High Availability active-passive clusters and software-defined WAN rules to ensure continuous network resilience.
- Audit firewall access rules and NAT change requests against NCA Control 7-4 documentation criteria.

Target Audience:

- You configure and administer perimeter firewall appliances within enterprise networking environments.
- You maintain security access controls and monitor intrusion alerts within operational security teams.
- You deploy network infrastructure and establish branch connectivity within systems engineering departments.
- You audit firewall rule changes and verify technical baseline compliance within information security divisions.



Course Outline:

Day 1: Configuring FortiGate Network Interfaces and Routing

- Deploying FortiOS interfaces using standard NAT and transparent modes
- Configuring static routes and administrative distances for gateway uplinks
- Managing administrative access rights and role-based profiles in FortiOS
- Configuring local network services and dynamic host configuration daemons
- Build: Initial FortiGate Interface Routing and Administrative Access Baseline

Day 2: Implementing Firewall Policies and Security Fabric

- Structuring firewall policies using defined source and destination objects
- Implementing central SNAT and DNAT pools for inbound mappings
- Integrating Fortinet Security Fabric telemetry across connected network assets
- Documenting firewall policy rule changes using NCA Control 7-4
- Build: Enterprise Firewall Policy and Security Fabric Access Matrix

Day 3: Deploying Unified Threat Management Security Profiles

- Configuring deep SSL inspection profiles using internal enterprise certificates
- Deploying antivirus and intrusion prevention signatures for perimeter defence
- Enforcing web filtering categories and domain name system protections
- Applying application control sensors to restrict unapproved enterprise software
- Build: Unified Threat Inspection and Content Filtering Profile Architecture

Day 4: Configuring Virtual Private Networks and High Availability

- Building route-based IPsec site-to-site VPN tunnels with automated failover
- Provisioning remote-access SSL VPN portals with multi-factor user authentication
- Configuring High Availability active-passive clusters for fault-tolerant operation
- Orchestrating SD-WAN traffic steering rules across multiple internet interfaces
- Build: Redundant Site-to-Site VPN and High Availability Cluster Template

Day 5: Executing Advanced Lab Operations and Compliance Audits

- Diagnosing packet drops using FortiOS command line packet sniffers
- Partitioning administrative resources and tenant routing using virtual domains
- Executing six-monthly firewall rule reviews per CSCC-1:2019 benchmark criteria
- Hardening FortiOS system settings against unauthorized administrative configuration modifications
- Build: FortiGate Network Security Infrastructure and Policy Baseline



Skills You Will Gain:

- FortiOS Interface Configuration
- Perimeter Firewall Rule Engineering
- Security Profile Threat Inspection
- Route-Based IPsec Tunnel Provisioning
- SSL VPN Remote Portal Administration
- High Availability Cluster Management
- SD-WAN Performance Path Steering
- Firewall Rule Change Compliance Auditing

Why Attend This Course:

- Build an operational FortiGate Network Security Infrastructure and Policy Baseline that you can directly apply to secure your production network.
- Master essential FortiOS configuration commands and graphical controls to deploy stateful access rules and unified threat management profiles.
- Establish redundant network topologies using FortiGate High Availability clustering and performance-based SD-WAN traffic steering rules.
- Align firewall rule management and NAT modification procedures with formal governance frameworks including NCA Control 7-4.

Conclusion:

On your first week back, you will use the FortiGate Network Security Infrastructure and Policy Baseline to assess your organisation's existing firewall policies and interface bindings. You will present the validated security profiles, high availability configurations, and change documentation templates to your network operations manager and chief information security officer. After initial implementation, you will check FortiGate session logs and packet sniffer outputs to verify that network traffic conforms precisely to established security boundaries without service degradation.

Frequently Asked Questions FAQ:

What will you be able to do after the FortiGate Administrator Training Course?

You will be able to deploy, configure, and maintain FortiGate firewalls running FortiOS. You can construct resilient firewall policies, integrate threat management profiles, establish IPsec and SSL VPNs, manage High Availability clusters, and diagnose connectivity anomalies using administrative diagnostic tools.



What do you need to know before starting the FortiGate Administrator Training Course?

You need a solid understanding of fundamental networking concepts, including IPv4 addressing, subnetting, TCP/IP protocol operations, and basic routing mechanics. Familiarity with general network security principles is recommended, though previous operational experience with Fortinet hardware is not required.

What do you build during the FortiGate Administrator Training Course?

You build a complete FortiGate Network Security Infrastructure and Policy Baseline. This deliverable includes configured interface routing, segmented access rules, content inspection profiles, site-to-site IPsec tunnels, an active-passive High Availability cluster, and an audit-ready rule change log.

How does the FortiGate Administrator Training Course differ from a course on a neighbouring subject or at another level?

This course focuses directly on the practical administration and security operations of FortiGate appliances using FortiOS. Unlike generic network security overviews or advanced architecture courses, this training delivers practitioner-level configuration competencies across daily operational firewall tasks, resilience clustering, and compliance record-keeping.

