BLACKBIRD FOR TRAINING

Network Firewall and Security

21 – 25 December 2026
London (UK)



Network Firewall and Security

Ref: 3255319_192652 **Date:** 21 – 25 December 2026 **Location:** London (UK) **Fees:** 6100 GBP

Introduction

In today's digital era, protecting network infrastructure from cyber threats is vital for business continuity and data integrity. Whether in enterprise environments, cloud systems, or data centers, effective firewall management and network security are the foundation of operational resilience and information protection.

This comprehensive training course provides participants with both the theoretical knowledge and hands-on technical skills required to secure networks effectively.

It is designed for IT professionals, network administrators, and security officers responsible for implementing and maintaining secure digital environments. Through real-world examples and lab-based exercises, participants will learn how to design, configure, and manage firewall systems and defense mechanisms that safeguard organizational networks.

Course Objectives

By the end of this course, participants will be able to:

- Understand the core principles of network and cybersecurity.
- Configure, monitor, and manage firewalls to protect against internal and external threats.
- Implement intrusion detection and prevention systems to identify and stop network attacks.
- Analyze network traffic and logs to detect suspicious activity.
- Develop and enforce effective network security policies.
- Apply hands-on firewall configuration and monitoring in simulated environments.
- Build proactive defense strategies for evolving cyber threats.

Course Outlines

Day 1: Network Security Fundamentals

- Introduction to cybersecurity principles and threat types.
- Understanding firewall concepts and their role in network protection.
- Cyber threat landscape: malware, phishing, and social engineering.
- Risk assessment and security policy development.
- Access control and authentication fundamentals.
- Practical exercise: creating a basic firewall policy.



Day 2: Firewall Architecture and Deployment

- Network segmentation and DMZ configuration.
- Packet filtering and access control mechanisms.
- Virtual Private Network VPN setup and remote access security.
- Traffic monitoring and event logging.
- Using analysis tools to identify anomalies.
- Lab: firewall rule creation and configuration testing.

Day 3: Advanced Firewall Management

- Understanding stateful vs. next-generation firewalls.
- Network Address Translation NAT and secure routing.
- Firewall performance tuning and optimization.
- High availability and redundancy concepts.
- Managing firewall updates and firmware security.
- Practical lab: designing multi-layer firewall protection.

Day 4: Intrusion Detection and Threat Prevention

- Fundamentals of IDS and IPS systems.
- Configuring and managing alerts for network events.
- Detecting and mitigating malware and denial-of-service attacks.
- Correlating events from multiple sources for threat intelligence.
- Using logs for forensic analysis and response planning.
- Lab: simulate a cyber-attack and implement response controls.

Day 5: Incident Response and Security Governance

- Network security best practices and compliance frameworks.
- Building and implementing security incident response plans.
- Policy enforcement and continuous monitoring.
- Reporting and documentation of security incidents.
- Final hands-on assessment: designing a secure network model.
- Review, discussion, and certification guidance.



Why Attend This Course? Wins & Losses!

- Gain practical expertise in firewall management and network security.
- Strengthen your ability to defend against real-world cyber threats.
- Enhance your technical credibility in IT security operations.
- Improve operational efficiency and network stability.
- Ensure compliance with global cybersecurity standards.
- Develop skills that are in high demand across industries.
- Experience real-world simulations and hands-on problem-solving.
- Build a foundation for advanced security certifications.

Conclusion

The Network Firewall and Security course empowers professionals with the essential tools and knowledge to protect modern networks against evolving cyber threats.Combining theory with extensive hands-on training, the program ensures participants can design, implement, and manage secure network infrastructures aligned with global security best practices.

By completing this course, participants will gain the technical expertise and confidence to enhance organizational resilience, minimize risk, and ensure long-term digital security.

