



TRAINING OFFERING

You can reach us at:

Arrow ECS, Nidderdale House, Beckwith Knowle, Harrogate, HG3 1SA

Email: educationteam.ecs.uk@arrow.com

Phone: 0870 251 1000



FCP - FortiGate Security & Infrastructure bundle

CODE:	LENGTH:	PRICE:
FNT_FT-FGT-SEC_INF	40 Hours (5 days)	£2,995.00

Description

This course has now been replaced with the 4-day FortiGate Administrator course.

If you have any questions, please call 0870 251 1000 or email educationteam.ecs.uk@arrow.com

In this course, you will learn how to use the most common FortiGate features, including security profiles and FortiGate networking and infrastructure features.

In interactive labs, you will explore firewall policies, the Fortinet Security Fabric, user authentication, and how to protect your network using security profiles, such as IPS, antivirus, web filtering, application control, and more.

These administration fundamentals will provide you with a solid understanding of how to implement basic network security.

For the Infrastructure part of the course, topics include features commonly applied in complex or larger enterprise or MSSP networks, such as advanced routing, redundant infrastructure, virtual domains (VDOMs), zero trust network access (ZTNA), SSL VPN, site-to-site IPsec VPN, single sign-on (SSO), and diagnostics.

Product Version

- FortiOS 7.2

Objectives

After completing this course, you will be able to:

- Deploy the appropriate operation mode for your network
- Use the GUI and CLI for administration
- Control network access to configured networks using firewall policies
- Apply port forwarding, source NAT, and destination NAT
- Authenticate users using firewall policies
- Understand encryption functions and certificates
- Inspect SSL/TLS-secured traffic to prevent encryption used to bypass security policies
- Configure security profiles to neutralize threats and misuse, including viruses, torrents, and inappropriate websites
- Apply application control techniques to monitor and control network applications that might use standard or non-standard protocols and ports
- Fight hacking and denial of service (DoS)
- Collect and interpret log entries
- Identify the characteristics of the Fortinet Security Fabric
- Analyze a FortiGate route table
- Route packets using policy-based and static routes for multipath and load-balanced deployments

- Divide FortiGate into two or more virtual devices, each operating as an independent FortiGate, by configuring virtual domains (VDOMs)
- Understand the fundamentals and benefits of using ZTNA
- Offer an SSL VPN for secure access to your private network
- Establish an IPsec VPN tunnel between two FortiGate devices
- Implement a meshed or partially redundant VPN
- Diagnose failed IKE exchanges
- Offer Fortinet Single Sign-On (FSSO) access to network services, integrated with Microsoft Active Directory (AD)
- Deploy FortiGate devices as an HA cluster for fault tolerance and high performance
- Diagnose and correct common problems

Audience

Who Should Attend

Networking and security professionals involved in the management, configuration, administration, design, implementation, and monitoring of FortiGate devices used to secure their organizations' networks should attend this course.

Prerequisites

- Knowledge of network protocols
- Knowledge of OSI layers
- Knowledge of firewall concepts in an IPv4 network

Programme

Security: 1. Introduction and Initial Configuration 2. Firewall Policies 3. Network Address Translation 4. Firewall Authentication 5. Logging and Monitoring 6. Certificate Operations 7. Web Filtering 8. Application Control 9. Antivirus 10. Intrusion Prevention and Denial of Service 11. Security Fabric Infrastructure:

- Routing
- Virtual Domains
- Fortinet Single Sign-On
- ZTNA
- SSL VPN
- IPsec VPN
- High Availability
- Diagnostics

Test and Certification

This course is intended to help you prepare for the NSE 4 certification exam: https://training.fortinet.com/local/staticpage/view.php?page=nse_4 Exam vouchers are available separately at an additional charge.

Session Dates

On request. Please [Contact Us](#)

Additional Information

This training is also available as onsite training. Please contact us to find out more.