Enterprise Computing Solutions - Education Services

TRAINING OFFERING

You can reach us at:

Arrow ECS, Woluwedal 30, 1932 Sint-Stevens-Woluwe

Email: education.ecs.benelux@arrow.com
Phone: +32 2 332 19 57

FCSS - Enterprise Firewall Administrator

CODE:	LENGTH:	PRICE:
FNT_FT-EFW	24 Hours (3 days)	Request Price

Description

In this course, you will learn how to implement, troubleshoot, and centrally manage an enterprise security infrastructure composed of multiple FortiGate devices.

Objectives

After completing this course, you will be able to:

- Integrate FortiManager, FortiAnalyzer, and multiple FortiGate devices using the Fortinet Security Fabric
- Centralize the management and monitoring of network security events
- Optimize FortiGate resources
- Diagnose and monitor user traffic using FortiGate debug tools
- Troubleshoot issues with conserve mode, high CPU, firewall policies, session helpers, IPsec, FortiGuard, content inspection, routing, and HA
- Harden the enterprise services
- Simultaneously deploy IPsec tunnels to multiple sites using the FortiManager VPN console
- Configure ADVPN to enable on-demand VPN tunnels between sites
- Combine OSPF and BGP to route the enterprise traffic

Audience

Networking and security professionals involved in the design, administration, and support of an enterprise security infrastructure using FortiGate devices.
This course assumes advanced knowledge of networking, and extensive hands-on experience working with FortiGate, FortiManager, and FortiAnalyzer.

Prerequisites

You must have an understanding of the topics covered in the following courses, or have equivalent experience:

- NSE 4 FortiGate Security
- NSE 4 FortiGate Infrastructure

It is also recommended that you have an understanding of the topics covered in the following courses, or have equivalent experience:

- NSE 5 FortiManager
- NSE 5 FortiAnalyzer

Programme

1. Security Fabric
2. FortiOS Architecture
3. Traffic and Session Monitoring
4. Routing
5. FortiGuard
6. High Availability

7. Central Management
8. OSPF
9. Border Gateway Protocol (BGP)
10. Web Filtering
11. Intrusion Prevention System (IPS)
12. IPsec
13. Autodiscovery VPN (ADVPN)

Further Information

If you take the online format of this class, you must use a computer that has the following:
A high-speed internet connection
An up-to-date web browser
A PDF viewer
Speakers or headphones
HTML 5 support
You should use a wired Ethernet connection, not a WiFi connection. Firewalls, including Windows Firewall or FortiClient, must allow connections to the online labs.

Session Dates

On request. Please Contact Us

Additional Information

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