# ARROW

## Enterprise Computing Solutions - Education Services

# TRAINING OFFERING

---

**Du kan nå os her**

.

Email: training.ecs.dk@arrow.com
Phone: +45 7025 4500

# NSE 6 FortiMail Email Filtering

| CODE: | LENGTH: | PRICE: |
|---|---|---|
| FNT_FMAIL | 24 Hours (3 dage) | Request Price |

## Description

In this 3-day class, you will learn how to use FortiMail 5.x.

In interactive labs, you will explore FortiMail's role as a specialized device, and how its features extend beyond FortiGate email filtering to provide both high-performance and in depth security for business-critical communications.

You will analyze MMS and email security challenges that administrators from small businesses to carriers face. These administrative fundamentals will provide you with a solid understanding of where and how to deploy and troubleshoot FortiMail, including FortiSandbox integration.

| | Method |
|---|---|
| | Instructor-led classroom |
| **Product Version** | Instructor-led online* |
| FortiMail 5.3 | Self-paced online |

**Certification**

This course prepares you for the FortiMail Specialist Exam. This course is part of preparation for the NSE 6 certification exam.

## Objectives

After completing this course, you will be able to:

- Integrate FortiMail with FortiSandbox
- Use FortiMail flexibly &emdash; for secure webmail and calendar, a shield for Microsoft Exchange, or as an ISP for clean pipes
- Deploy HA & redundant infrastructure for ultimate uptime of mission-critical email
- Protect the priceless reputation of your MTA on spam blacklists
- Secure email transmission via best-of-breed technologies: SMTPS, SMTP over TLS, S/MIME, and IBE
- Archive email for compliance
- Leverage your existing LDAP / Active Directory server for user preferences & authentication
- Eliminate spear phishing, leaks, & zero-day viruses
- Throttle client connections, blocking MTA abuse
- Understand the system architecture of a FortiMail appliance: how email flows through its modules, how it applies intelligent routing and policies to email, and what parts of the configuration to check if legitimate email is being detected as spam
- Block spam with sophisticated techniques: deep header inspection, heuristics, recipient verification, PDF/image scans, third-party DNSBL and SURBL queries, and the FortiGuard Antispam service

## Prerequisites

Experience with email servers (SMTP) Basic understanding of network security

## Programme

1.Email Concepts
2.Basic Setup
3.Server Mode
4.Access Control
5.SSL/TLS
6.Session Monitoring
7.Antivirus & Content Inspection
8.Antispam
9.IBE
10.High Availability
11.Gateway & Transparent Mode
12.Diagnostics

## Session Dates

På anmodning. Kontakt os venligst

## Yderligere Information

Denne træning er også tilgængelig som træning på stedet. Kontakt os for at finde ud af mere.