FortiMail

In this three-day class, you will learn how to use FortiMail to protect your network from existing email-borne threats, as well as use FortiSandbox to detect and block emerging threats.

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 email security challenges that administrators of small businesses and carriers face, and learn where and how to deploy, manage, and troubleshoot FortiMail.

Product Version

FortiMail 5.3.8

Formats

- Instructor-led classroom
- Instructor-led online*
- Self-paced online

*Private class only. Contact your Fortinet sales representative for more information.

Agenda

1 Email Concepts
2 Basic Setup
3 Access Control and Policies
4 Authentication
5 Session Management
6 Antivirus and Content Inspection
7 Antispam
8 Securing Communications
9 High Availability
10 Server Mode
11 Transparent Mode
12 Maintenance and Troubleshooting

Objectives

After completing this course, you should be able to:

- Position FortiMail in an existing or new email infrastructure using any of the flexible deployment modes
- Understand the system architecture of FortiMail: how email flows through its modules; how it applies intelligent routing and policies to email; and how it can protect the priceless reputation of your message transfer agent (MTA)
- Use your existing LDAP server to manage and authenticate users
- Secure email transmission using best-in-class technologies such as SMTPS, SMTP over TLS, and Identity Based Encryption
- Throttle client connections to block MTA abuse

- Block spam using sophisticated techniques such as deep header inspection, spam outbreak, heuristics, and the FortiGuard Antispam service
- Eliminate spear phishing and zero-day viruses
- Integrate FortiMail with FortiSandbox for advanced threat protection
- Prevent accidental or intentional leaks of confidential and regulated data
- Archive email for compliance
- Deploy high availability (HA) and redundant infrastructure for maximum uptime of mission-critical email
- Diagnose common email and FortiMail-related issues

*This course covers gateway and server mode in depth. This course also covers transparent mode, however, if you require a course on the use of transparent mode in carrier environments, you should order customized training.

Who Should Attend

Networking and security professionals involved in the administration and support of FortiMail.

Prerequisites

- Basic understanding of TCP/IP networking and network security concepts
- Experience with SMTP, PKI, SSL/TLS, RADIUS, and LDAP is recommended

System Requirements

To take this course online, your computer must have the following:

- High-speed Internet connection
- Up-to-date web browser
- PDF viewer
- Speakers or headphones
- HTML 5 support

You should use a wired Ethernet connection, *not* a Wi-Fi connection. *Firewalls, including Windows Firewall or FortiClient, must allow connections with the online labs*.

Certification

This course prepares you for the FortiMail 5.3.8 specialist exam. This is one of the courses that prepares you to take the NSE 6 certification exam.