FORTINET CERTIFIED PROFESSIONAL
Public Cloud Security

FORTINET
Authorized
Premier Training Center

FortiMail

In this course, you will analyze email security challenges that administrators face, and learn where and how to deploy, manage, and troubleshoot FortiMail to protect your network from email-borne threats. You will also explore the role of FortiMail as a specialized device, and how its features provide both high-performance and in-depth security for business-critical communications.

Product Version

FortiMail 7.2

Course Duration

- Lecture time (estimated): 10 hours
- Lab time (estimated): 10 hours
- Total course duration (estimated): 20 hours
  - 3 full days or 5 half days

Who Should Attend

Security professionals involved in the management, configuration, administration, and monitoring of FortiMail in small to enterprise deployments should attend this course.

Certification

This course is intended to help you prepare for the *Fortinet - NSE 6 FortiMail 7.2* certification exam. This exam is part of the Fortinet Certified Professional - Public Cloud Security certification track.

Prerequisites

You must have an understanding of the topics covered in *FCP - FortiGate Security* and *FCP - FortiGate Infrastructure*, or have equivalent experience.

It is also recommended that you have an understanding of the following topics:

- SMTP
- PKI
- SSL/TLS
- LDAP

Agenda

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

Objectives

After completing this course, you will 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 (IBE)
- 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 (ATP)
- Prevent accidental or intentional leaks of confidential and regulated data
- Archive email for compliance
- Deploy high availability (HA) and redundant infrastructure for maximum up-time of mission-critical email
- Diagnose common issues related to email and FortiMail

NOTE: 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.

Training Delivery Options and SKUs

Instructor-Led Training

Includes standard NSE training content delivered in person onsite, or live online using a virtual classroom application. Training is delivered within public classes or as a private class. Private requests are scoped, quoted, developed, and delivered by Fortinet Training (minimum quantities apply).

Use the following ILT Training SKU to purchase scheduled public classes of this course through Fortinet Resellers or Authorized Training Partners:

FT-FML

Self-Paced Training

Includes online training videos and resources through the Fortinet Training Institute library, free of charge.

You can purchase on-demand lab access with interactive, hands-on activities using the following methods:

- Credit card, through the course on the Fortinet Training Institute
- Purchase order (PO), through Fortinet Resellers or Authorized Training Partners

After you complete the purchase, you receive lab access and the accompanying lab guide within the self-paced course.

Use the following on-demand lab training SKU to purchase lab access using a PO:

FT-FML-LAB

See Purchasing Process for more information about purchasing Fortinet training products.

(ISC)²

- CPE training hours: 10
- CPE lab hours: 10
- CISSP domains: Communications and Network Security

Program Policies and FAQs

For questions about courses, certification, or training products, refer to Program Policy Guidelines or Frequently Asked Questions.