FORTINET
NSE Training Institute

Course Description

FortiMail

In this three-day class, you will learn how to use FortiMail to protect your network from email-borne threats, and you will learn how to integrate with FortiSandbox to detect and block advanced persistent threats.

In interactive labs, you will 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.

You will analyze email security challenges that administrators face, and learn where and how to deploy, manage, and troubleshoot FortiMail.

Product Version

FortiMail 6.4

Formats

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

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 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 (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

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

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

Prerequisites

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

System Requirements

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
- One of the following:
  - HTML5 support
  - An up-to-date Java Runtime Environment (JRE) with Java plugin enabled in your web browser

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

Certification

This course is intended to help participants prepare for the *NSE 6 FortiMail* certification exam.