FORTINET
Premier Authorized Training Center

fast lane

FORTINET CERTIFIED PROFESSIONAL
Public Cloud Security

FortiMail

Course Description

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:

3 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

Outlines:

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