



FortiMail Email Filtering Course 221-v2.0

Course Overview

FortiMail Email Filtering is a 2-day instructor-led course with comprehensive hands-on labs to provide you with the skills needed to configure, manage and maintain a FortiMail Secure Messaging Platform.

The course begins by discussing the email security challenges that many enterprises face. Students then learn through hands-on experience how to configure the product features that provide protection against these threats. Antispam, antivirus, content inspection and email archiving capabilities are all thoroughly explored.

Also included, is an overview of the SMTP protocol and a detailed look at FortiMail email traffic flow. Through the use of policies and profiles, students configure optimized protection against advanced email attacks. Operational maintenance and real-time network solutions (FortiGuard Subscription Services) are discussed, and at the end of the course students will configure a high availability active-passive group.

Participants gain a solid understanding of how to integrate a FortiMail Secure Messaging appliance into their existing email infrastructure and the configuration required to successfully remove unwanted spam, provide maximum protection for blended email-related threats and facilitate regulatory compliance.

Course Objectives

Upon completion of this course, students will be able to:

- Use the GUI and CLI to perform administration and maintenance functions for the FortiMail security appliance including system backups, routing and domain configuration, HA failover setup, antispam quarantine management and report generation.
- Protect valuable corporate MTA processing resources by validating recipients and blocking messages to invalid users using recipient verification capabilities.



- Configure policies to apply inspection and protection profiles for ongoing corporate email security and the enforcement of email policy.
- Understand the system architecture of a FortiMail appliance, how email flows through it, and how it applies intelligent routing and policies to message traffic.
- Configure protection profiles for multi-layered antivirus, antispam, and antispymware security protection.
- Use system session profiles to set mail client connection thresholds and cut-off MTA accessibility to spammers.
- Configure archiving features to comply with best practices email archiving guidelines.
- Deploy antispam filtering techniques including deep header inspection, heuristics, image scan, banned words, third-party DNSBL and SURBL servers and the FortiGuard Antispam Service.
- Configure antivirus filtering profiles to apply antivirus scanning and remove viruses and spyware embedded in email.

Prerequisites

- Basic knowledge of email and SMTP

Who Should Attend

This course is intended for anyone who is planning, implementing and administrating the FortiMail Secure Messaging platform.



Course Topics

Module 1 – FortiMail Overview

- What is FortiMail?
- Email Basics
- FortiMail Operating Modes
 - Transparent Mode
 - Gateway Mode
 - Server Mode

Module 2 – System and Mail Settings

- Admin Access
- Network Settings
- Logging and Reporting
- Mail Settings
- Access Lists
- Recipient Address Verification
- Deferred Delivery and Delivery Status Notification
- Customized Messages - Disclaimers
- Map or Alias Email Addresses
- Domain Administration

Module 3 – Policies and Profiles

- Policies and Profiles Defined
- Benefits of Policies and Profiles
- Recipient Based Policies
- IP Based Policies
- When to use IP Policies?
- Policy Check – How it works?
- Policy Rules
- Authentication Options

Module 4 – Antispam Profiles

- FortiMail Mail Analysis Flow
- Spam Detection
- Session Based Antispam Techniques
 - Session Rate Limiting



- Sender Reputation
- Protocol Check
- Unauth Sessions
- SMTP Errors
- Recipient Address Check
- Greylisting and IP Blacklisting
- Application Level Antispam
 - FortiGuard Antispam Service (DNSBL, SURBL, SHASH)
 - Forged IP Scanning
 - Deep Header Scanning
 - Greylist Filtering
 - Image Analysis Filtering
 - Local Reputation Filtering
 - Heuristics
 - Per User/ Domain Bayesian Filtering
 - Black/White Lists
 - Banned Words/Dictionary Scanning
- Spam Handling

Module 5 – Antivirus and Content Profiles

- Virus Detection
- Content Filtering
- Attachment Filtering
- Dictionary Profile Set-up

Module 6 – Email Archive

- Email Archiving
- Archiving Policy and Exempt Policy
- Email Archive Access

Module 7 – Administration

- Maintenance
 - Firmware Upgrade
 - FortiGuard Subscription Services
 - Full System Backups
- Troubleshooting
 - CLI Commands for Network Connectivity Testing
 - Mail Queues
 - Mail History



Module 8 – High Availability

- FortiMail High Availability
- HA Active-Passive Mode
- Synchronizing Mail Data
 - System Mail Directory
 - User Home Directories
 - MTA Spool Directories
- HA Service Monitor
- HA Config-only
- HA Network Interface Configuration
- HA Implementation