

FortiMail Email Filtering

Course Number 9222 – 24 Hours

Overview:

FortiMail Email Filtering is an 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 is designed for FortiMail v4.0.

The course begins by discussing the email security challenges that many enterprises face.

Through hands-on experience students then learn how to configure the product features that provide protection against these threats. Antispam, Antivirus, Content Inspection, Email Archiving and Quarantine capabilities are all thoroughly explored and students get

a detailed look at FortiMail email traffic flow. Through the use of policies and profiles, students configure optimized protection against advanced email attacks.

Also included, is an in depth look and practical application of using SMTP authentication, PKI authentication, SMTPS, TLS and S/MIME for providing authentication and securing mail communications. Students create and use LDAP profiles for recipient address and domain verification, user authentication and automatic removal of invalid quarantine accounts.

Operational maintenance and real-time network solutions (FortiGuard Subscription Services) are discussed, and students have an opportunity to experiment with various FortiMail unit diagnostics commands and hardware troubleshooting techniques.

At the end of the course, students will configure a high availability active-passive group then set up a FortiMail appliance in Server mode to provide an all-in-one SMTP server solution that encompasses Antispam and Antivirus capabilities.

By the completion of this course, participants of FortiMail Email Filtering will gain a solid understanding of how to integrate a FortiMail Secure Messaging appliance into their existing email infrastructure in order to provide maximum protection against blended email-related threats and facilitate regulatory compliance.

Audience:

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

Prerequisites:

- Attendees of this course must possess a basic knowledge of email and SMTP.

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 Antispyware 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.
- Integrate the FortiMail unit to an existing LDAP directory to dynamically retrieve specific configuration data.
- Regulate the usage of company resources and secure the data transmission by using best of breed technologies such as SMTPS, SMTP over TLS and S/MIME.
- Maximize the configurations of the three operational modes (Server, Transparent and Gateway) to fulfill any business requirement.

Certifications:

This course helps to prepare students for the following certification exams:

- Fortinet Certified FortiMail Security Specialist (FCFSS)

Course content:

- Lesson 1 – FortiMail Introduction
 - FortiMail Security Appliances
 - Identifying Email Risks and Solutions
 - Summary of FortiMail Benefits
 - FortiMail Operating Modes
 - Mail Message Flow
 - FortiMail and FortiGate Feature Comparison
- Lesson 2 - System Configuration
 - Administration Interfaces
 - FortiMail Network Configuration
 - System Administrators
 - FortiMail Logging
 - Reports

- SNMP
- Lesson 3 - Email Setup
 - FortiMail Email Handling
 - Email Domain
 - Configuring a Protected Domain
 - Hostname and Local Domain
 - Email User Management
 - User Alias and Address Map
 - Managing Mail Storage and Mail Queues
- Lesson 4 - Policies and Profiles
 - Access Control Rules
 - Delivery Rules
 - Policy Types
 - Profiles
- Lesson 5 – Antispam
 - FortiMail Antispam Techniques
 - FortiGuard Antispam Service
 - Antispam Profiles
 - Order of Execution of Antispam Techniques
 - X-FEAS Tags
 - Comparing FortiMail and FortiGate Antispam Techniques
 - FortiMail Antispam Usage Recommendations
- Lesson 6 - Session Monitoring
 - Configuring Session Profiles
- Lesson 7 - Antivirus and Content Scanning
 - FortiMail Antivirus Protection
 - Antivirus Profile
 - Content Filtering Overview
 - Content Profile
 - Attachment Filtering
 - File Type Filtering
 - Scan Conditions
 - Content Monitoring and Filtering
- Lesson 8 - Email Archiving and Quarantine
 - Email Archiving
 - Configuring Email Archiving
 - Email Archiving and Exemption Policies
 - Managing Archived Email
 - Email Quarantine
 - User Quarantine Preferences
 - System Quarantine
 - Quarantine Report
 - User Access to Quarantine
- Lesson 9 - Authentication and Securing Communications
 - SMTP Authentication
 - PKI Authentication

- FortiMail PKI Support
- SMTPS (Secure SMTP)
- SMTP over Transport Layer Security (TLS)
- TLS Profile
- S/MIME
- Lesson 10 - LDAP
 - LDAP Profile
 - User Query
 - Recipient Address Verification
 - Automatic Removal of Invalid Quarantine Accounts
 - Domain Verification
 - Group Query
 - User Authentication
 - User Alias
 - Mail Routing
 - Advanced LDAP Profile Settings
- Lesson 11 – Diagnostics
 - General Problem Description
 - Storage Structure
 - System Information
 - Hardware Troubleshooting
 - Backups
 - Troubleshooting Commands
 - Log Analysis
- Lesson 12 - Transparent Mode
 - Configuring Network Interfaces
 - Deployment Scenarios
 - Transparent Mode Options
 - Transparent Mode Mail Flow
- Lesson 13 - High Availability
 - Introduction
 - HA Deployment Modes
 - Configuration Share (Config-only) Mode
 - Active-Passive Mode
 - Implementing HA
 - Active-Passive Settings
 - Config-Only Mode Settings
 - Active Passive Data Synchronization
 - Heartbeat Parameters
 - Service Monitor
 - HA Status Monitoring
- Lesson 14 - Server Mode
 - Users and User Groups
 - Resource Profiles
 - Global Address Book
 - Mail Storage