FortiMail Email Filtering

Course 221 (for FortiMail v5.0)

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. 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, S/MIME and IBE 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 set up a FortiMail appliance in Server mode to provide an all-in-one SMTP server solution that encompasses antispam and antivirus capabilities by populating the user list from an LDAP server.

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.
Course Objectives

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

- Use the FortiMail unit’s web UI and CLI to perform administration and maintenance functions 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 with 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, S/MIME and IBE.
- Maximize the configurations of the three operational modes (Server, Transparent and Gateway) to fulfill any business requirement.
Products Used in This Course
- FortiMail

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

Who Should Attend
This course is intended for anyone who is planning, implementing and administrating a FortiMail Secure Messaging platform.

Certification
This course helps to prepare students for the following certification exam:
- Fortinet Certified Email Security Professional (FCESP)

Course Topics

AGENDA - Day 1

FortiMail Overview
- Summary of FortiMail Key Benefits
- FortiMail Operating Modes
- FortiMail Family of Security Appliances
- Email Basics Overview
- Mail Message Flow

System Configuration
- Administration Interfaces (web UI and CLI)
- FortiMail Network Configuration
- System Administrators
- FortiMail Logging
- Reports
- SNMP
Email Setup
- FortiMail Email Handling
- Email Domain
- Configuring a Protected Domain
- Recipient Verification
- Quarantine Management
- Domain Association
- Email User Management
- User Alias and Address Map
- Managing Mail Storage and Mail Queues

Access Control and Inspection
- Policies and Profiles
- Access Receive Rules
- Policy Types
  - Recipient Based Policies
  - IP-Based Policies

Antispam
- FortiMail Antispam Techniques
- Fortinet FortiGuard Antispam Service
- Session Based and Application Based Inspection
- Antispam Profiles
- Antispam Techniques
- Bounce Address Tag Configuration
- Black/White Lists
- X-FEAS Tags

Session Monitoring
- Configuring Session Profiles
- Sender and Endpoint Reputation
- Sender Validation (DKIM)
- SMTP Limits and Error Handling
- Header Manipulation
Content Inspection and Archiving
- Virus Detection
- Antivirus Profile
- Content Profile Usage
  - Attachment Filtering
  - File Type Filtering
  - Content Monitoring Inspection
  - Content Based Encryption
  - Defer Delivery of Email Messages
- Email Archiving
  - Archive Accounts
  - Email Archiving and Exemption Policies
  - Managing Archived Email

AGENDA - Day 2

Securing Communications
- Email Trends and Privacy Concerns
- SMTP Authentication
  - Recipient-Based Authentication
  - IP-Based Authentication
  - Access Control Receive Rules
- SMTPS (Secure SMTP)
- SMTP over Transport Layer Security (TLS)
- TLS Profile
- S/MIME
- Identity Based Encryption (IBE)
  - Secure Mail Delivery Methods (Pull and Push)
  - IBE Secure Portal
  - IBE User Management
LDAP
  • LDAP Profile
  • User Query
    o Group Query
    o User Authentication
    o User Alias
    o Mail Routing
    o Address Mapping
    o Recipient Address Verification
    o Automatic Removal of Invalid Quarantine Accounts
    o Domain Verification
  • Advanced LDAP Settings

Maintenance and Troubleshooting
  • FortiMail Storage Structure
  • System Information and Performance
  • Resource Usage
  • Network Statistics
  • RAID
  • Mail Statistics
  • Backups
  • Troubleshooting Commands and Packet Sniffer
  • FortiGuard Update Service
  • Troubleshooting Basics (logs, false positives, SMTP timeouts etc.)

Transparent Mode
  • Transparent Mode Advantages
  • Configuring Network Interfaces
    o Bridge and Route Mode
  • Deployment Scenarios
  • Transparent Mode Options
  • Transparent Mode Mail Flow and Inspection
  • Built-in MTA
ForiMail High Availability
  • FortiMail HA Introduction
  • HA Deployment Modes
    o Configuration Share (Config-only) Mode
    o Active-Passive Mode
  • Implementing HA
    o Active-Passive Settings
    o Config-Only Mode Settings
    o Active Passive Data Synchronization
    o Heartbeat Parameters
    o HA Service Monitor
  • HA Status Monitoring
  • Firmware Upgrade Procedure

Server Mode
  • Server Mode Introduction
  • Users and User Groups
  • Domain-Level Framework
  • Mail Data Migration
  • Resource Profiles
  • Mail Storage
    o NAS Configuration
  • User Account Management
  • Groupware Functionalities
  • Webmail Calendar and Built-in Agenda
  • Calendar Sharing
  • Address Book Management and Access Control
    o Personal Address Book
    o Global Address Book
    o Per Domain Address Book
  • Address Book LDAP Synchronization
  • FortiMail LDAP Address Book