



FortiMail™

Comprehensive Email Security



FortiMail

FortiMail 60D, 200D, 400C, 1000D, 3000C and 3000D

Comprehensive Email Security

Proven Security

FortiMail appliances and virtual appliances are proven, powerful email security platforms for any size organization — from small businesses to carriers, service providers, and large enterprises. Purpose-built for the most demanding messaging systems, FortiMail appliances employ Fortinet’s years of experience in protecting networks against spam, malware, and other message-borne threats.

Intelligent Protection

FortiMail prevents your email systems from becoming threat delivery systems. Its inbound filtering engine blocks spam and malware before it can clog your network and affect users. Its outbound inspection technology prevents other antispam gateways from blacklisting your users by blocking outbound spam and malware, including mobile traffic.

Key Features & Benefits

| | |
|---|--|
| Flexible Deployment Options | FortiMail can be deployed in gateway, transparent mode and as a fully featured mail server. With hardware, VM and cloud form factors, FortiMail is flexible enough to cater to every customer requirement. |
| Apply Data Loss Prevention and Identity-Based Encryption | Detect sensitive information using defined data patterns and ensure secure delivery with no additional hardware or software to install, no user provisioning, no recipient pre-enrollment. |
| Prevent Phishing and Other Advanced Threats | Apply embedded URL inspection, top rated antimalware and optional sandbox integration to detect highly targeted attacks. |
| Identify and Block Spamming Endpoints | Carriers and Service Providers, prevent blacklisting of legitimate subscribers by identifying and blocking endpoints sending spam. |
| No Per-User or Per-Mailbox Pricing | Complete, multi-layered antivirus, antispam, antispysware and antiphishing protection for an unlimited number of users. Greatly reduces TCO. |

Comprehensive Email Security

- Scalable solution from SME to the largest ISP and carrier networks
- Advanced Threat Outbreak Protection methods to protect against new emerging and targeted attacks
- Apply Identity-Based Encryption in both push and pull methods
- Data Leak Prevention, and Policy-Based Encryption and Archiving enable compliance with SOX, GLBA, HIPAA, PCI DSS
- Enforce email and security policies at a granular level
- Receive real-time security updates from FortiGuard® Services
- Industry leading price/performance
- Flexible deployment modes and architectures support the widest range of organizations
- Multi-layer threat detection delivers highest level of user protection
- Scalable solution delivers long term investment protection



Enforce secure content delivery with FortiMail Identity-Based Encryption (IBE), S/MIME, or TLS email encryption options. Prevent accidental and intentional loss of confidential data using predefined HIPAA, GLBA, SOX or customized dictionaries.

High Performance and Unmatched Flexibility

FortiMail appliances provide high-performance email routing and security by utilizing multiple high-accuracy antispam filters. When coupled with industry leading real-time antivirus and antispymware protection from FortiGuard Services, FortiMail provides you with extremely fast and accurate email security that won't affect end users or delay their communications. FortiMail can be deployed in the cloud or on premises and gateway, inline and server modes in a range of appliance or virtual machine form factors. This flexibility allows you to deploy FortiMail in the mode that best suits your environment.

FEATURES

System

- Transparent, Gateway and Server Mode Deployment Options
- Flexible Interface Configuration Including VLAN and Redundant Interface Support
- Inbound and Outbound Inspection
- Multiple Email Domains with Domain Level Customization
- IPv6 and IPv4 Address Support
- Virtual Hosting using Source and/or Destination IP Address Pools
- Policy-Based Mail Archiving with Remote Storage Options
- SMTP Authentication Support via LDAP, RADIUS, POP3 and IMAP
- LDAP-Based Email Routing
- Per User Inspection using LDAP Attributes on a Per Policy (Domain) Basis
- Comprehensive Webmail Interface for Server Mode Deployments and Quarantine Management
- Mail Queue Management
- Multiple Language Support for Webmail and Admin Interface
- Email RFC Compliance
- Maintains Local Sender Reputation List Based on:
 - Sender Policy Framework (SPF)
 - Domain Keys Identified Mail (DKIM)

Management, Logging, and Reporting

- QuickStart Setup Wizard
- Basic / Advanced Management Modes
- Role-Based Administration Accounts Per Domain
- Comprehensive activity and incident logging and reporting
- Configuration Change and Management Event Logging
- Built-in Reporting module
- Centralized logging and reporting with FortiAnalyzer
- Centralized Quarantine for large scale deployments
- SNMP Support using Standard and Private MIB with Threshold-Based Traps
- External or Local Storage Server Support, including iSCSI devices
- External Syslog support

High Availability (HA)

- Supported in all Modes
- Active-Passive Mode
- Configuration Synchronization Mode (Configuration Master and Slave Mode)
- Quarantine and Mail Queue Synchronization
- Device Failure Detection and Notification
- Link Status, Failover and Redundant Interface Support

Advanced Threat Protection

In addition to FortiGuard antivirus, FortiMail supports on-board code emulation to identify and block suspicious files based on their intended behavior. Optional cloud-based or on-premise “sandboxing” provide a full, contained, run-time environment to thwart the highly targeted and tailored attacks that increasingly bypass traditional defenses. Rich threat intelligence, actionable insight and the option to share information with FortiGuard Labs in order to receive automated protection updates help organizations reduce the risk of compromise and breach from such sophisticated attacks.

Antispam Profile

- FortiGuard Antispam Service
 - Global Sender Reputation
 - Spam and phishing URIs and email addresses
 - Spam Object checksums
 - Dynamic Heuristic Rules
- Outbreak Protection
- Greylisting for IPv4, IPv6 addresses and email accounts
- Local Sender Reputation (IPv4, IPv6 and End Point ID-based)
- Behavioral Analysis
- Deep Email Header Inspection
- Flexible Action and Notification Profiles
- Third party Spam URI and Real-Time Blacklists (SURBL/RBL)
- Full category FortiGuard URL Filtering
- Quarantining, tagging and end user reporting
- PDF Scanning and Image Analysis
- Black/White Lists at Global, Domain, and User levels
- Bayesian Statistic Filtering
- Newsletter detection

FEATURES

Antivirus

- FortiGuard Antivirus Service
- Quarantine, Repackage, Replace, and Monitor Actions
- Nested Archive Scanning
- Malware Detection
- On-board code emulation
- Integration with FortiSandbox and FortiGuard Analytics for advanced threat protection
 - Emails are queued by FortiMail whilst FortiSandbox inspects the email contents for threats

Content-Based Protection

- Dictionary-based filtering in inbound or outbound direction
- Predefined HIPAA, GLBA and SOX dictionaries
- Filter by Attachment File Type
- Banned Word Filtering

Denial-of-Service Protection

- Inbound and Outbound Message Rate Limiting
- Recipient Address Attack
- Reverse DNS Check (Anti-Spoofing)
- Forged Sender Address

Encryption

- Identity-based Encryption for Push/Pull Delivery of Encrypted Messages
- S/MIME Support for Gateway-to-Gateway Encryption
- Support for strong-crypto protocols including HTTPS, SMTPS, SSH, IMAPS and POP3S

Server Mode Specific Features

- SMTP, IMAP, and POP3 Email Services
- SMTP over SSL Support
- Disk Quota Policy Support for User Accounts
- Secure WebMail Client Access
- User, Group and Alias List Support
- Local Account and LDAP Authentication
- WebMail Calendar
- Email Auto Reply and Forwarding Preference
- Address Book Synchronize with LDAP

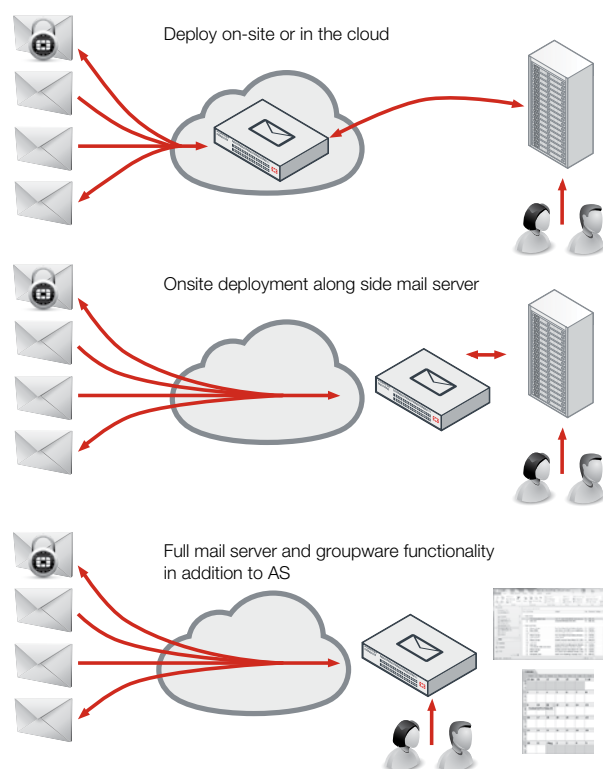
DEPLOYMENT

Choose from three modes of deployment — Transparent, Gateway, or Server mode – to meet your specific email security requirements, while minimizing infrastructure changes and service disruptions:

Gateway Mode: Provides inbound and outbound proxy mail transfer agent (MTA) services for existing email gateways. A simple DNS MX record change redirects email to FortiMail for antispam and antivirus scanning. The FortiMail device receives messages, scans for viruses and spam, then relays email to its destination email server for delivery.

Transparent Mode: Each network interface includes a proxy that receives and relays email. Each proxy can intercept SMTP sessions even though the destination IP address is not the FortiMail appliance. FortiMail scans for viruses and spam, then transmits email to the destination email server for delivery. This eliminates the need to change the DNS MX record, or to change the existing email server network configuration.

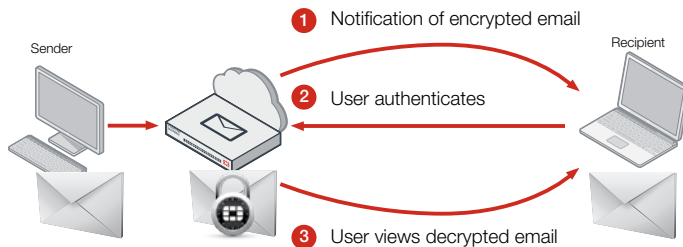
Server Mode: The FortiMail device acts as a stand-alone messaging server with full SMTP email server functionality, including flexible support for secure POP3, IMAP and WebMail access. FortiMail scans email for viruses and spam before delivery. As in Server mode, external MTAs connect to FortiMail, allowing it to function as a protected server.



DEPLOYMENT

Identity-Based Encryption (IBE)

IBE allows FortiMail to deliver confidential and regulated email securely — without requiring additional hardware, software user provisioning, or extra license fees. Use IBE to eliminate paper-based communications and reduce costs.



Policy-Based Encryption: Automatically encrypt messages for compliance, based on content or recipient.

Push or Pull Mode: Use Push, Pull, or a combination of modes to meet your requirements.

Easy to Deploy, Use, and Manage: Deploy IBE in any mode, including Transparent mode, without user provisioning or additional hardware or software.

SPECIFICATIONS

| | FORTIMAIL 60D | FORTIMAIL 200D | FORTIMAIL 400C |
|---|---|--|--|
| Suggested Deployment Scenarios | Demo, testing, training and small enterprise use with fewer than 100 users* | Small businesses, branch offices, and organizations with fewer than 400 users* | Small-to-midsized organizations with up to 1000 users* |
| Hardware Specifications | | | |
| 10/100/1000 Interfaces (Copper, RJ-45) | 4 | 4 | 4 |
| SFP Gigabit Ethernet Interface | 0 | 0 | 0 |
| Redundant Hot Swappable Power Supplies | No | No | No |
| Storage | 1x 500 GB | 1x 1 TB | 2x 1 TB |
| RAID Storage Management | No | No | Software: 0, 1 |
| Form Factor | Desktop Appliance | Rack Mount Appliance | Rack Mount Appliance |
| System Specification | | | |
| Configured Domains ** | 2 | 20 | 100 |
| Recipient-based Policies (per Domain / per System) — Incoming or Outgoing | 15 / 30 | 60 / 300 | 600 / 3000 |
| Server Mode Mailboxes | 50 | 150 | 400 |
| Antispam, Antivirus, Authentication, and Content Profiles (per Domain / per System) | 10 / 15 | 50 / 60 | 50 / 200 |
| Performance (Messages/Hour) [Without queuing based on 100 KB message size] | | | |
| Email Routing | 3.6 K | 76 K | 150 K |
| FortiGuard Antispam | 3.1 K | 68 K | 140 K |
| FortiGuard Antispam + Antivirus | 2.7 K | 58 K | 120 K |
| Dimensions | | | |
| Height x Width x Length (inches) | 1.61 x 8.27 x 5.24 | 1.75 x 17.05 x 13.86 | 1.70 x 17.10 x 14.30 |
| Height x Width x Length (mm) | 41 x 210 x 133 | 45 x 433 x 352 | 44 x 435 x 364 |
| Weight | 2.6 lbs (1.2 kg) | 13.4 lbs (6.1 kg) | 16.1 lbs (7.3 kg) |
| Environment | | | |
| Power Source | External Power Supply 19V DC 2.1A 40 W | | 100–240V AC, 50–60 Hz |
| Maximum Power Required | 20 W | 1.00A / 110V, 0.50A / 220V | 4.00A / 110V, 2.00A / 220V |
| Power Consumption (Average) | 24 W | 60 W | 100 W |
| Heat Dissipation | 78 BTU/h | 205 BTU/h | 342 BTU/h |
| Humidity | 10–90% non-condensing | 5–95% non-condensing | 10–90% non-condensing |
| Operating Temperature | 32–104°F (0–40°C) | 32–104°F (0–40°C) | 32–104°F (0–40°C) |
| Storage Temperature | -13–158°F (-25–70°C) | -13–158°F (-25–70°C) | -4–158°F (-20–70°C) |
| Compliance | FCC Part 15 Class B, C-Tick, VCCI, CE, UL/cUL, CB | FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB | |
| Certification | | VBSspam and VB100 rated | VBSspam and VB100 rated, Common Criteria EAL 2+, FIPS 140-2 Validation |

* Suggested sizing for Gateway and Transparent deployments. For Server Mode, see Server Mode Mailbox metric. If unsure, please validate the model selection by checking the peak mail flow rates and average message size detail with a FortiMail specialist.

** Configured domains is the total number of email domains that can be configured on the appliance. Domain Associations can be used to enable additional domains which share configuration with the primary domain to which they are assigned.

SPECIFICATIONS

| | FORTIMAIL 1000D | FORTIMAIL 3000C | FORTIMAIL 3000D |
|---|--|--|---|
| Suggested Deployment Scenarios | | | |
| | Mid to large enterprise, education and government departments with up to 3000 users* | Universities, Large enterprise, ISP, Carrier | Highest performing appliance for the largest University, corporate, ISP and carrier customers |
| Hardware Specifications | | | |
| 10/100/1000 Interfaces (Copper, RJ-45) | 6 | 4 | 4 |
| SFP Gigabit Ethernet Interface | 2 | 2 | 2 |
| Redundant Hot Swappable Power Supplies | Yes | Yes | Yes |
| Storage | 2x 2 TB (2x 2 TB Optional) | 2x 1 TB (4x 1 TB Optional) | 2x 2 TB (6x 2 TB Optional) |
| RAID Storage Management | Hardware: 1, 5, 10, 50, Hot Spare (Based on Drive Count) | Hardware: 1, 5, 10, 50, Hot Spare (Based on Drive Count) | Hardware: 1, 5, 10, 50, Hot Spare (Based on Drive Count) |
| Form Factor | Rack Mount Appliance | Rack Mount Appliance | Rack Mount Appliance |
| System Specification | | | |
| Configured Domains ** | 800 | 2000 | 2000 |
| Recipient-Based Policies (per Domain / per System) — Incoming or Outgoing | 1,500 / 7,500 | 1,500 / 7,500 | 1,500 / 7,500 |
| Server Mode Mailboxes | 1500 | 3000 | 3000 |
| Antispam, Antivirus, Authentication, and Content Profiles (per Domain / per System) | 50 / 600 | 50 / 600 | 50 / 600 |
| Performance (Messages/Hour) [Without queuing based on 100 KB message size] | | | |
| Email Routing | 680 K | 900 K | 1.2 M |
| FortiGuard Antispam | 620 K | 830 K | 1.1 M |
| FortiGuard Antispam + Antivirus | 500 K | 730 K | 1.0 M |
| Dimensions | | | |
| Height x Width x Length (inches) | 3.46 x 17.24 x 14.49 | 3.46 x 17.40 x 29.00 | 3.46 x 18.99 x 29.00 |
| Height x Width x Length (mm) | 88 x 438 x 368 | 88 x 442 x 737 | 88 x 482 x 737 |
| Weight | 57.5 lbs (26.1 kg) | 50.0 lbs (22.7 kg) | 71.5 lbs (32.5 kg) |
| Environment | | | |
| Power Source | 100–240V AC, 50–60 Hz | | |
| Maximum Power Required | 3.50A / 110V, 1.75A / 220V | 7.0A / 110V, 3.5A / 220V | 10.0A / 110V, 5.0A / 220V |
| Power Consumption (Average) | 115 W | 200 W | 340 W |
| Heat Dissipation | 471 BTU/h | 683 BTU/h | 1160 BTU/h |
| Humidity | 5–95% non-condensing | 5–95% non-condensing | 20–90% non-condensing |
| Operating Temperature | 32–104°F (0–40°C) | 50–95°F (10–35°C) | 50–95°F (10–35°C) |
| Storage Temperature | -13–158°F (-25–70°C) | -40–149°F (-40–65°C) | -40–149°F (-40–65°C) |
| Compliance | | | |
| | FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB | FCC Part 15 Class A, C-Tick, VCCI, CE, BSMI, KC, UL/cUL, CB, GOST | |
| Certification | | | |
| | VBSspam and VB100 rated | VBSspam and VB100 rated, Common Criteria EAL 2+, FIPS 140-2 Validation | VBSspam and VB100 rated |

* Suggested sizing for Gateway and Transparent deployments. For Server Mode, see Server Mode Mailbox metric. If unsure, please validate the model selection by checking the peak mail flow rates and average message size detail with a FortiMail specialist.

** Configured domains is the total number of email domains that can be configured on the appliance. Domain Associations can be used to enable additional domains which share configuration with the primary domain to which they are assigned.



FortiMail 60D



FortiMail 200D



FortiMail 400C



FortiMail 1000D



FortiMail 3000C



FortiMail 3000D

SPECIFICATIONS

| Technical Specifications for FortiMail Virtual Appliances | VM00 | VM01 | VM02 | VM04 | VM08 |
|---|---|--|---|--|------------------|
| Suggested Deployment Scenarios | Demo, testing, training and small enterprise use with fewer than 100 users* | Small businesses, branch offices, and organizations with fewer than 400 users* | Small to midsize organizations with up to 1000 users* | Mid to large enterprise with up to 3000 users* | Large enterprise |
| Technical Specifications | | | | | |
| Hypervisors Supported | VMware ESXi / ESX 4.0 / 4.1 / 5.0 / 5.1 / 5.5 | | | | |
| Virtual Machine Form Factor | Open Virtualization Format (OVF) | | | | |
| Maximum Virtual CPUs Supported | 1 | 1 | 2 | 4 | 8 |
| Virtual NICs Required (Minimum/Maximum) | 1 / 4 | 1 / 4 | 1 / 4 | 1 / 4 | 1 / 4 |
| Virtual Machine Storage Required (Minimum/Maximum) | 50 GB / 1 TB | 50 GB / 1 TB | 50 GB / 2 TB | 50 GB / 4 TB | 50 GB / 8 TB |
| Virtual Machine Memory Required (Minimum/Maximum) | 1 GB / 2 GB | 1 GB / 2 GB | 1 GB / 4 GB | 1 GB / 8 GB | 1 GB / 16 GB |
| Performance (Messages/Hour) [Without queuing based on 100 KB message size]** | | | | | |
| Email Routing | 3.6 K | 34 K | 67 K | 306 K | 675 K |
| FortiGuard Antispam | 3.1 K | 30 K | 54 K | 279 K | 630 K |
| FortiGuard Antispam + Antivirus | 2.7 K | 26 K | 52 K | 225 K | 585 K |
| System Specifications | | | | | |
| Configured Domains *** | 2 | 20 | 100 | 800 | 2000 |
| Recipient-Based Policies (Domain / System) — Incoming or Outgoing | 15 / 30 | 60 / 300 | 600 / 3,000 | 1,500 / 7,500 | 1,500 / 7,500 |
| Server Mode Mailboxes | 50 | 150 | 400 | 1500 | 3,000 |
| Antispam, Antivirus, Authentication, and Content Profiles (per Domain / per System) | 10 / 15 | 50 / 60 | 50 / 200 | 50 / 600 | 50 / 600 |

* Suggested sizing for Gateway and Transparent deployments. For Server Mode, see Server Mode Mailbox metric. If unsure, please validate the model selection by checking the peak mail flow rates and average message size detail with a FortiMail specialist.

** Hardware dependent. Indicative figures based on multiple VMs running on a shared system.

*** Configured domains is the total number of email domains that can be configured on the appliance. Domain Associations can be used to enable additional domains which share configuration with the primary domain to which they are assigned.

ORDER INFORMATION

| Product | SKU | Description |
|-----------------|----------------|---|
| FortiMail 60D | FML-60D | Email Security Appliance — 4x GE RJ45 ports, 500 GB storage. |
| FortiMail 200D | FML-200D | Email Security Appliance — 4x GE RJ45 ports, 1 TB storage. |
| FortiMail 400C | FML-400C | Email Security Appliance — 4x GE RJ45 ports, 2 TB storage. |
| FortiMail 1000D | FML-1000D | Email Security Appliance — 2x GE SFP slots, 6x GE RJ45 ports, dual AC power supplies, 4 TB default storage. |
| FortiMail 3000C | FML-3000C-E02S | Email Security Appliance — 2x GE SFP slots, 4x GE RJ45 ports, dual AC power supplies, 2 TB default storage. |
| FortiMail 3000D | FML-3000D | Email Security Appliance — 2x GE SFP slots, 4x GE RJ45 ports, dual AC power supplies, 4 TB default storage. |

FortiMail 60D not available for sale in North America.



GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA SALES OFFICE
Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel: 011-52-(55) 5524-8480