

# FortiMail™

## Comprehensive Messaging Security



### Proven Security

FortiMail appliances and virtual appliances are proven, powerful messaging 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 messaging 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. FortiMail dynamic and static user-blocking gives you granular control over all of your email policies and users.

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 FortiMail predefined 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 antispayware protection from FortiGuard Services, FortiMail provides you with extremely fast and accurate messaging security that won’t affect end users or delay their communications. Deploy messaging security in the mode that best suits your environment and users with FortiMail’s unmatched flexibility.

### Comprehensive Messaging Security

- ✓ Inspect more than 2 million emails per hour
- ✓ Unmatched deployment flexibility
- ✓ Apply Identity-Based Encryption in both push and pull methods
- ✓ Use customized and predefined dictionaries to prevent data loss
- ✓ Enforce email and security policies at a granular level
- ✓ Receive real-time security updates from FortiGuard® Services



Features	Benefits
<b>Deploy appliances or virtual appliances in Transparent, Gateway, or Server modes</b>	All email servers on the market deploy in Server mode, some offering a Gateway mode option. Fortinet is the only vendor to offer Transparent mode, enabling FortiMail to intercept emails without changing DNS MX records, or existing email server network configurations.
<b>Apply Identity-Based Encryption in both push and pull methods</b>	Ensures secure delivery of confidential or regulated content. Extremely easy to deploy – no additional hardware or software to install, no user provisioning, no pre-enrollment for recipient.
<b>Data Loss Prevention and Compliance</b>	Detect accidental or intentional loss of confidential or regulated data. Achieve PCI-DSS or HIPAA compliance by blocking messages containing defined data patterns, or creating policies to enforce encryption of certain emails.
<b>Identify and Block Spamming Endpoints</b>	Prevent blacklisting of legitimate subscribers by identifying and blocking endpoints sending spam, including Smart phones. Ideal for Carriers and Service Providers.
<b>No per-user or per-mailbox pricing</b>	Complete, multi-layered antivirus, antispam, antispayware and anti-phishing protection for an unlimited number of users. Greatly reduces TCO.

## TRANSPARENT, GATEWAY AND SERVER MODE FEATURES

- Multiple Email Domain Support
- High Availability (HA) Support
- SMTP Mail Gateway for Existing Email Servers
- Integrated Policy-Based Email Routing and Queue Management
- Outbound Mail Relay for Improved Mail Security
- Granular Layered Detection Policies for Spam and Viruses Addresses, IP Addresses, or Domains
- Per User Antivirus and Antispam Scanning Using LDAP Attributes on a Per Policy (Domain) Basis
- LDAP-Based Email Routing
- Quarantined Message Access with WebMail and POP3
- Daily Quarantine Summaries
- Policy-Based Archiving of Inbound and Outbound Messages with Backup Support for Remote Storage
- Mail Queue Support for Failed, Deferred, and Undeliverable Email
- SMTP Authentication Support Through LDAP, RADIUS, POP3 or IMAP
- Per User Automatic White List
- SNMP Support Using Standard and Private MIB with Threshold Based Traps
- Maintains Local Sender Reputation List Based on:
  - Number of Viruses Sent
  - Amount of Spam Sent
  - Number of Bad Recipients
- Dynamic DNS (DDNS)
- Greylist Database Persistence
- Security Hardened Operating System
- Multiple Language Support
- Regex Pattern Matching
- Sender Policy Framework (SPF)
- DomainKeys
- DomainKeys Identified Mail (DKIM)
- Fragmented Message Blocking
- Virtual Host Support Using Pool of IP Address for Source and/or Destination

## DENIAL-OF-SERVICE PROTECTION

- Denial of Service (Mail Bombing)
- Recipient Address Attack
- Email Rate Limiting
- 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

## HIGH AVAILABILITY (HA)

- Supported in all Modes
- Active-Passive Configuration
- Quarantine and Mail Queue Synchronization
- Stateful Failover
- Device Failure Detection and Notification
- Link Status Monitor
- Link Failover

## MANAGEMENT, LOGGING, AND REPORTING

- QuickStart Setup Wizard
- Basic / Advanced Management Modes
- Real-time Statistics
- Tiered Administration Accounts
- Quarantine Search Capability
- Automated PDF report scheduling
- Configuration Change and Management Event Logging
- Antivirus Incident Logging
- Antispam Activity Logging
- External or Local Syslog Server Support
- External or Local Storage Server Support, Including iSCSI devices
- Expanded Central Reporting with FortiAnalyzer Support
- Critical Events and Virus Incident Alerting
- Comprehensive Reporting with Over 140 Reports In Seven Categories
- Scheduled Report Generation
- Dictionary-triggered Archiving

## ANTISPAM - CONTENT LEVEL DETECTION

- Inbound and Outbound Filtering
- Extensive Heuristic Spam Filters
- Dynamic Heuristic Rule Updates
- Attachment/Content Filtering
- Deep Email Header Inspection
- Bayesian Statistic Filtering
- Spam URI Real-Time Blocklists (SURBL)
- Banned Word Filtering
- Inbound and Outbound Filtering
- Spam Quarantining and Spam Tagging
- Spam Management (Accept, Relay, Reject or Discard) Based on Email SHASH Spam Checksum Block List
- Spam Image Analysis Scanning
- PDF Scanning / PDF Image Scanning
- FortiGuard Antispam Service
- Global and User Customized Black/White Lists
- 3rd Party Real-Time Black Listed (RBL) Support
- Forged IP Checking
- Greylist Checking

## ANTIVIRUS / ANTISPYWARE PROTECTION

- Virus Scan SMTP Messages
- Compressed Attachment and Nested Archive Support
- Quarantine Infected Files
- Replacement Message Notification
- Block by File Type
- Attachment Filtering

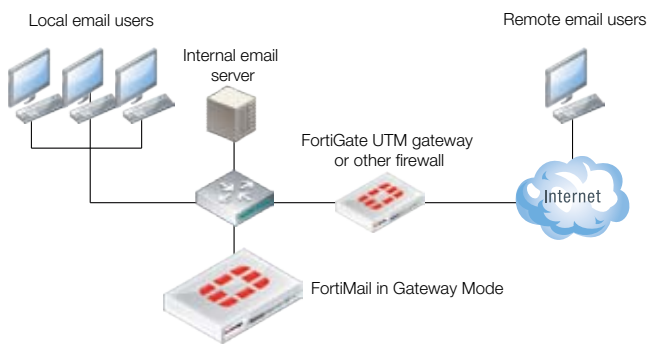
## SERVER MODE SPECIFIC FEATURES

- POP3, SMTP, and IMAP 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
- Bulk Folder Support for Spam Mail
- WebMail Calendar
- Email Forwarding Preference
- Address Book Synchronize with LDAP

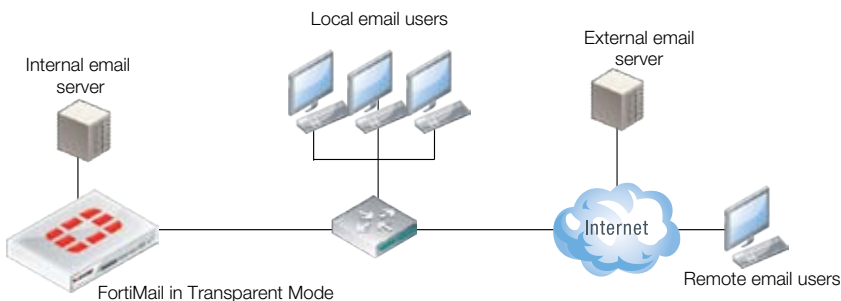
## FortiMail Deployment Options

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

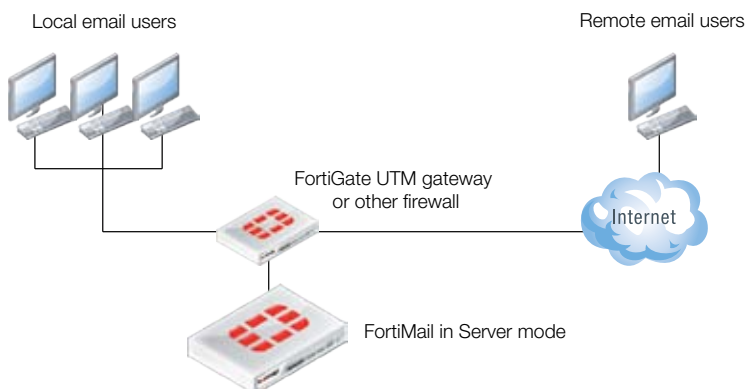
- Gateway Mode:** Provides inbound and outbound proxy mail transfer agent (MTA) services for existing email gateways. A simple DNS MX record change redirects email to FortiMail for antispam and antivirus scanning. The FortiMail device receives messages, scans for viruses and spam, then relays email to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

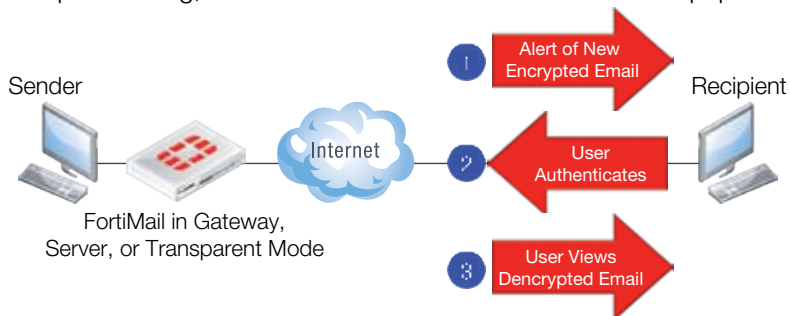


- Server Mode:** The FortiMail device acts as a stand-alone messaging server with full SMTP email server functionality, including flexible support for secure POP3, IMAP and WebMail access. FortiMail scans email for viruses and spam before delivery. As in Server mode, external MTAs connect to FortiMail,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



## 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.



Technical Specifications	FortiMail-100C	FortiMail-400B	FortiMail-2000B	FortiMail-3000C	FortiMail-5002B
<b>Hardware Specifications</b>					
10/100 Interfaces (Copper, RJ-45)	1	0	0	0	0
10/100/1000 Interfaces (Copper, RJ-45)	2	4	6	4	3
SFP Gigabit Ethernet Interface	0	0	0	2	0
Internal Backplane Base / Fabric Channel Interfaces	0	0	0	0	2 / 2
Expansion Slot	0	0	0	0	0
Redundant Hot Swappable Power Supplies	No	No	Yes	Yes	N/A
Storage	1 TB	1 x 500 GB (1 TB Optional)	2 x 1 TB (6 TB Optional)	2 x 1 TB (6 TB Optional)	1x 146GB HDD (RTM Module included)
RAID Storage Management	No	Software: 0, 1 (Raid 1 Requires Second 500 GB Drive)	Hardware: 1, 5, 10, 50, Hot Spare (Based on Drive Count)	Hardware: 1, 5, 10, 50, Hot Spare (Based on Drive Count)	No
Form Factor	Desktop	Rack Mount Appliance	Rack Mount Appliance	Rack Mount Appliance	ATCA Chassis
<b>System Specifications</b>					
Email domains	50	500	5,000	5,000	10,000
Recipient based policies (per Domain / per System) - incoming or Outgoing	60 / 300	600 / 3000	1,500 / 7,500	1,500 / 7,500	1,500 / 7,500
Server Mode Mailboxes	200	1,000	3,000	3,000	3,000
Antispam, Antivirus, Authentication, and Content Profiles (per Domain / per System)	50 / 60	50 / 200	50 / 600	50 / 600	50 / 600
Unlimited User Licenses	Yes	Yes	Yes	Yes	Yes
<b>Performance (Messages/Hour) [Without queuing based on 3 KB message size]</b>					
Email Routing	90,000	300,000	1.5 Million	2.0 Million	2.3 Million
FortiGuard Antispam	85,000	280,000	1.3 Million	1.8 Million	2.2 Million
FortiGuard Antispam + Antivirus	80,000	250,000	1.2 Million	1.6 Million	2.0 Million
<b>Dimensions</b>					
Height x Width x Length (in)	1.75 x 15 x 6.3 in	1.7 x 17.3 x 14.5 in	3.4 x 17.4 x 26.8 in	3.4 x 17.4 x 26.8 in	1.2 x 11.0 x 12.2 in
Height x Width x Length (cm)	4.4 x 38 x 16 cm	4.5 x 43.8 x 36.8 cm	8.6 x 44.3 x 68.1 cm	8.6 x 44.3 x 68.1 cm	3 cm x 32 x 38 cm
Weight	4 lbs (1.8 kg)	10 lb (4.5 kg)	57.5 lb (26.1 kg)	57.5 lb (26.1 kg)	5.9 lb (2.68 kg)
<b>Environment</b>					
Power Required	100-240V AC	100-240V AC	100 – 240 V, 50/60 HZ, 7.0 – 3.5A	100 – 240 V, 50/60 HZ, 7.0 – 3.5A	-40.5 V (DC) to -57 V (DC)
Power Consumption (AVG)	56 W	121 W	152 W	200 W	148 W
Heat Dissipation	190.4 BTU	304 BTU	519 BTU	868 BTU	610 BTU
Operating Temperature	32 – 104 deg F (0 – 40 deg C)	32 – 104 deg F (0 – 40 deg C)	50 – 95 deg F (10 – 35 deg C)	50 – 95 deg F (10 – 35 deg C)	32 – 131 deg F (0 – 55 deg C)
Storage Temperature	-13 to 158 deg F (-35 to 70 deg C)	-13 to 158 deg F (-35 to 70 deg C)	-40 – 149 deg F (-40 – 65 deg C)	-40 – 149 deg F (-40 – 65 deg C)	-40 to 158 deg F (-40 to 70 deg C)
Humidity	5 to 95% non-condensing	5 to 95% non-condensing	5 to 95% non-condensing	5 to 95% non-condensing	5 to 93% non-condensing
<b>Compliance</b>					
	FCC Class A Part 15, CE Mark	FCC Class A Part 15, UL/CUL, C Tick, VCCI	FCC Class A, UL/CB/CUL, C Tick, VCCI, US EPA Energy Star Compliant	FCC Class A, UL/CB/CUL, C Tick, VCCI, US EPA Energy Star Compliant	FCC Class A Part 15, UL/CB/CUL
<b>Certifications</b>					
	VBSspam Platinum, Common Criteria EAL 2+, FIPS 140-2 Validation				FCC 47 CFR Part15, Class A, CE, UL60950-1/CSAC22.2

FortiMail Virtual Appliances	FortiMail-VM01	FortiMail-VM02
<b>Technical Specifications</b>		
Hypervisors Supported	VMware ESXi/ESX/4.0/4.1	VMware ESXi/ESX/4.0/4.1
Max vCPUs Supported	1	2
Max vNICs	4	4
Virtual Machine Storage (Min / Max)	50 GB / 1 TB	50 GB / 1 TB
Virtual Machine Memory Required (Min / Max)	1 GB / 2 GB	1 GB / 4 GB
<b>System Performance</b>		
Email Routing	90,000	265,000
FortiGuard Antispam	85,000	234,000
FortiGuard Antispam / Antivirus	77,000	185,400

FortiMail Virtual Appliances	FortiMail-VM01	FortiMail-VM02
<b>System Specifications</b>		
Email Domains	50	500
Recipient-based policies (Domain / System)	60 / 300	600 / 3000
Server Mode Mailboxes	200	1000
Profiles (Domain / System)	50 / 60	50 / 200
Unlimited User License	Yes	Yes

#### GLOBAL HEADQUARTERS

Fortinet Incorporated  
1090 Kifer Road, Sunnyvale, CA 94086 USA  
Tel +1.408.235.7700  
Fax +1.408.235.7737  
www.fortinet.com/sales

#### EMEA SALES OFFICE – FRANCE

Fortinet Incorporated  
120 rue Albert Caquot  
06560, Sophia Antipolis, France  
Tel +33.4.8987.0510  
Fax +33.4.8987.0501

#### APAC SALES OFFICE – SINGAPORE

Fortinet Incorporated  
300 Beach Road 20-01, The Concourse  
Singapore 199555  
Tel +65-6513-3734  
Fax: +65-6295-0015



Copyright© 2011 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, and FortiGuard®, are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance metrics contained herein were attained in internal lab tests under ideal conditions, and performance may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to the performance metrics herein. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any guarantees. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Certain Fortinet products are licensed under U.S. Patent No. 5,623,600.