



FortiMail™

Comprehensive Messaging Security

Proven Security

The FortiMail family of appliances is a proven, powerful messaging security platform for any size organization, from small businesses to carriers, service providers, and large enterprises. Purpose-built for the most demanding messaging systems, the FortiMail appliances utilize Fortinet's years of experience in protecting networks against spam, malware, and other message-borne threats.

Intelligent Protection

You can prevent your messaging systems from becoming threat delivery systems with FortiMail. Its inbound filtering engine blocks spam and malware before it can clog your network and affect users. Its outbound inspection technology prevents outbound spam or malware from causing other antispam gateways to blacklist your users (including 3G mobile traffic). FortiMail's dynamic and static user blocking gives you granular control over all of your policies and users.

Secure Content Delivery

FortiMail enables identity-based encryption (IBE) to ensure secure delivery of confidential or regulated content. IBE uses full public key encryption to encrypt messages for your customers, employees, or partners, without an additional cost. There is no additional hardware or software to install, no user provisioning, and no pre-enrollment for recipients, making it extremely easy to deploy.

You can enable automatic encryption of messages based on the attributes you choose, such as subject content, message body, or recipient domain. FortiMail IBE also offers the choice of push or pull delivery options, delivering encrypted emails directly to your users, or storing them on the FortiMail for retrieval, or a combination of the two options.

Data Loss Prevention

FortiMail includes customizable, predefined dictionaries that detect the accidental or intentional loss of confidential or regulated data. You can choose to block messages containing data matching a range of patterns, including credit card numbers, social security and social insurance numbers, and bank routing numbers. Alternatively, you can create policies to require the encryption of messages carrying this data.



FortiMail Product Family: Comprehensive Messaging Security

The FortiMail product line provides specialized messaging security system for organizations of all sizes. From remote or branch offices to global carriers, FortiMail platforms provide multi-layered protection against blended message-borne threats composed of spam, viruses, worms, phishing, and spyware.

The FortiMail family eliminates malicious and harmful content quickly and efficiently with its three antispam, antivirus, and antispyware filtering engines. By integrating certified spam and virus recognition methodologies, FortiMail has demonstrated the ability to block 99.87% of spam in live third-party tests. ICSA Labs certifies the accuracy of FortiMail's antispam engine.

FortiGuard® Security Subscription Services deliver dynamic, automated updates for antispam, antivirus, and antispyware security services.

Virus Bulletin awarded FortiMail its VBSpam Platinum Award, in recognition of FortiMail's high catch rate and low false positives.

Features

Benefits

Unmatched deployment flexibility

Deploy FortiMail in Transparent, Gateway, or Sever mode, to meet your specific messaging security requirements and minimize infrastructure changes or service disruptions

Integrated security with no per-user or per-mailbox pricing

Complete multi-layered antivirus, antispam, antispyware, and antiphishing security protection for an unlimited number of users

Antispam gateway that retrieves endpoint information

Enables Carriers and Service Providers to block spamming endpoints (including smartphones) preventing blacklisting of legitimate subscribers

Appliance or blade form-factor

Chose the right appliance or blade that fits your environment, including FortiGate-5000 series chassis or other ATCA-compliant chassis

Industry Certification



FortiMail Features

Fortinet's FortiMail Secure Messaging Systems are purpose-built antispam/antivirus systems that protect organizations against message-borne threats. They deliver a simple approach to securing and cleansing corporate messaging communications. The FortiMail systems provide high-performance mail routing and security by utilizing multiple high accuracy antispam filters. Coupled with FortiGuard™ Labs' industry leading real-time antivirus and antispyspware protection. FortiMail provides you with extremely fast and accurate messaging security that will not become a network bottleneck. FortiMail's high performance, coupled with its three deployment options and wide range of features, make it ideal for you to deploy in almost any environment.

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 Mibs 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

SERVER MODE SPECIFIC FEATURES

Supported in Server Mode Only:
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

HIGH AVAILABILITY (HA)

Supported for Gateway, Transparent, and Server Modes
Active-Passive Configuration
Quarantine and Mail Queue Synchronization
Stateful Failover
Device Failure Detection and Notification
Link Status Monitor
Link Failover

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

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

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 Blocklist
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

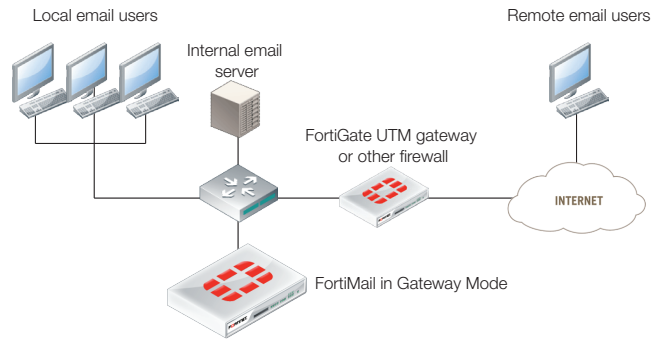
MANAGEMENT, LOGGING, AND REPORTING

Quick-Start 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

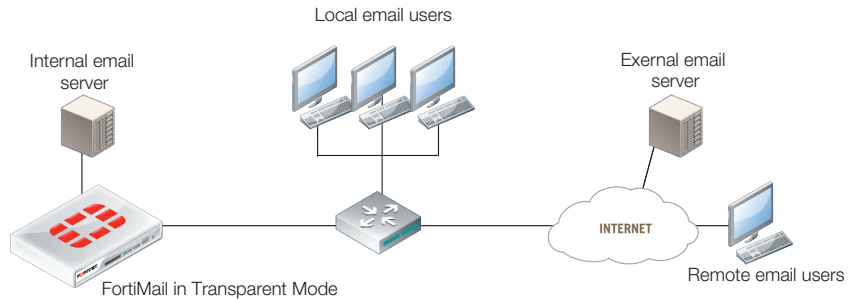
FortiMail Deployment Options

You have the option of deploying FortiMail in Transparent, Gateway, or Server mode, to meet your specific messaging security requirements and minimize infrastructure changes or service disruptions:

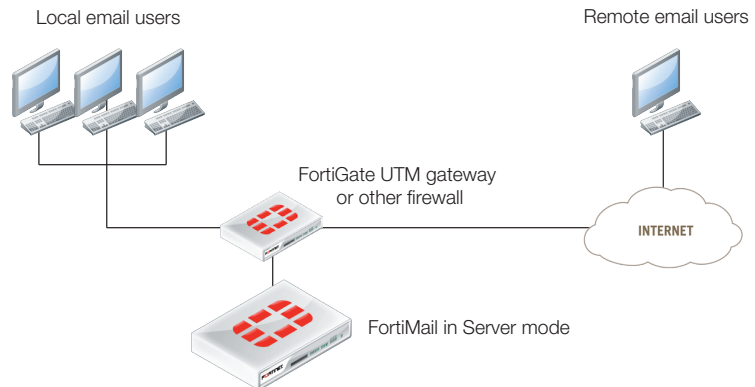
- Gateway Mode:** Provides inbound and outbound proxy mail transfer agent (MTA) services for existing email gateways. A simple DNS MX record change redirects email to FortiMail for antispam and antivirus scanning. The FortiMail unit receives messages, scans for viruses and spam, then relays email to 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 is not the FortiMail appliance. FortiMail scans for viruses and spam, and then transmits email to destination email server for delivery. Eliminates the need to change the DNS MX record or change the existing mail server network configuration.

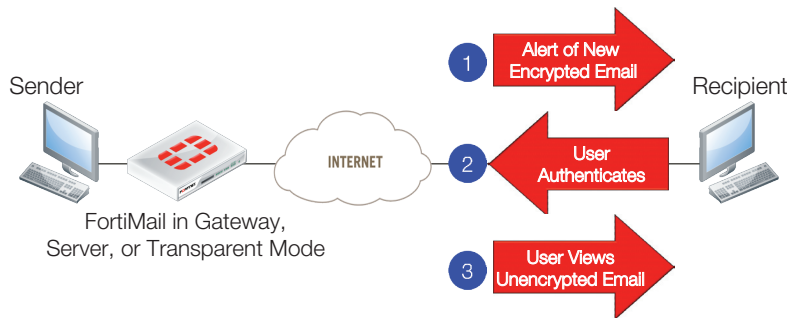


- Server Mode:** The FortiMail unit acts as a stand-alone messaging server and delivers full-featured SMTP mail server functionality, with flexible support for secure POP3, IMAP and WebMail access. It receives messages, scans for viruses and spam, and then delivers to its email users' mailboxes. External MTAs connect to the FortiMail server, as it is its own protected email server.



Identity Based Encryption

Deliver confidential or regulated email securely without requiring additional hardware, software user provisioning, or additional license fees. Eliminate the use of paper-based communications to save costs.



- Policy-Based Encryption:** Create policies to 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:** Implement IBE in any deployment mode, including Transparent. Deploy without any user provisioning or additional hardware or software



Technical Specifications	FortiMail-100C	FortiMail-400B	FortiMail-2000B	FortiMail-5001A
Hardware Specifications				
10/100 Interfaces (Copper, RJ-45)	1	0	0	0
10/100/1000 Interfaces (Copper, RJ-45)	2	4	6	2
Internal Backplane Base / Fabric Channel Interfaces	0	0	0	2 / 2
Expansion Slot	0	0	0	1 Single-Width AMC
Redundant Hot Swappable Power Supplies	No	No	Yes	N/A
Storage	1 TB	1 x 500 GB (1 TB Optional)	2 x 1 TB (6 TB Optional)	1 x 80 GB HDD (ASM Storage Module)
RAID Storage Management	No	Software: 0, 1 (Raid 1 Requires Second 500 GB Drive)	Hardware: 1, 5, 10, 50, Hot Spare (Based on Number of Drives)	No
Form Factor	Desktop	Rack Mount Appliance	Rack Mount Appliance	ATCA Chassis
System Specifications				
Email domains	50	500	5,000	10,000
Recipient based policies (per Domain / per System) - incoming or Outgoing	60 / 300	600 / 3000	1,500 / 7,000	1,500 / 7,000
Server Mode Mailboxes	200	1,000	3,000	3,000
Antispam, Antivirus, Authentication, and Content Profiles (per Domain / per System)	50 / 60	50 / 200	50 / 600	50 / 600
Unlimited User Licenses	Yes	Yes	Yes	Yes
Performance (Messages/Hour) [Without queuing based on 3 KB message size]				
Email Routing	90,000	264,600	1.1 Million	1.4 Million
FortiGuard Antispam	85,000	234,000	1.1 Million	1.3 Million
FortiGuard Antispam + Antivirus	77,000	185,400	1.0 Million	1.1 Million
Dimensions				
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	1.2 x 14.0 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	3 cm x 35.5 x 31 cm
Weight	4 lbs (1.8 kg)	10 lb (4.5 kg)	57.5 lb (26.1 kg)	8 lb (3.6 kg)
Environment				
Power Required	100-240V AC	100-240V AC	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	148 W
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)	32 – 104 deg F (0 – 40 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)	-31 to 158 deg F (-35 to 70 deg C)
Humidity	5 to 95% non-condensing	5 to 95% non-condensing	5 to 95% non-condensing	20 to 90% non-condensing
Compliance				
	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 Part 15, UL/CB/CUL, C Tick, VCCI
Certifications				
	ICSA Labs Antispam, VBSpam Platinum			

FortiGuard® Security Subscription Services deliver dynamic, automated updates for Fortinet products. The Fortinet Global Security Research Team creates these updates to ensure up-to-date protection against sophisticated threats. Subscriptions include antivirus, intrusion prevention, web filtering, antispam, vulnerability and compliance management, application control, and database security services.

FortiCare™ Support Services provide global support for all Fortinet products and services. FortiCare support enables your Fortinet products to perform optimally. Support plans start with 8x5 Enhanced Support with “return and replace” hardware replacement or 24x7 Comprehensive Support with advanced replacement. Options include Premium Support, Premium RMA, and Professional Services. All hardware products include a 1-year limited hardware warranty and 90-day limited software warranty.



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
61 Robinson Road, #09-04 Robinson Centre
Singapore 068893
Tel +65-6513-3730
Fax +65-6223-6784