



# FortiMail™

## 邮件安全

### 业内认可的安全产品

FortiMail硬件平台和虚拟机平台被证明是强大的邮件安全系统，能够有效地为大中型企业提供邮件安全防护。FortiMail凝聚了Fortinet多年防垃圾邮件、恶意软件和其他邮件类的攻击经验。

### 智能化的防护体系

FortiMail可以对发出的邮件进行垃圾邮件过滤，防止用户的邮件服务器成为攻击源。FortiMail能够处理垃圾邮件、病毒、蠕虫和间谍软件等多种威胁的专用反垃圾邮件设备。它采用优化的操作系统和专用防病毒和反垃圾邮件的引擎。

### 性能卓越，部署灵活

FortiMail实现了高性能的邮件路由，并且通过保护内容表的方式灵活地部署反垃圾邮件策略。FortiGuard为FortiMail提供了全球24×7的病毒库、入侵库和间谍软件库的升级服务。FortiMail部署灵活，能够在较低的拥有成本的前提下，实现双向的邮件路由、QoS控制和邮件归档等功能。

DATASHEET



### 强大的邮件安全

- ✓ 每小时监测200万以上邮件
- ✓ 部署极为灵活
- ✓ 无论是推送和拉送，都可以基于ID的加密99
- ✓ 用户自定义和预定义的字典实现数据防泄漏
- ✓ 细粒度地部署邮件和安全的策略
- ✓ 通过FortiGuard服务获取实时的升级



### 特点和益处

◇ 支持透明、路由、和服务器模式的邮件安全解决方案	目前市场的邮件服务器均是以服务器模式工作的，有些可选网关模式。Fortinet是唯一支持透明、路由和服务器模式的查您，这样部署 FortiMail时就不需要修改 DNS MX 记录。
◇ 可以部署基于 ID 的加密	确保数据传送的机密程度，易于部署——不需要附加的软件和硬件，也不需要根据用户和接收者来确定。
◇ 数据防泄漏和符合法规要求	监测是否有机密数据意外地或者故意地外泄，通过部署根据关键词和创建强制策略加密重要邮件，以满足 PCIDSS 和 HIPAA 的要求
◇ 识别和阻断发送垃圾邮件的终端用户	识别和阻断终端用户发送垃圾邮件而导致公司被列入黑名单，这也支持智能手机，非常适合于运营商和服务商
◇ 按设备收取费用，不再按用户收费	不限用户地支持反垃圾邮件、防病毒、反钓鱼、反间谍软件等功能，能够有效地降低用户的总体成本

## 透明、网关和服务器模式的通用功能

支持多个邮件域  
多个管理员  
高可用性  
SMTP 邮件网关  
基于策略的邮件路由和队列管理  
流出的邮件中继  
基于每用户的防病毒、反垃圾邮件策略  
基于 LDAP 的邮件路由  
通过 Web Mail 和 POP3 的邮件隔离区  
每天隔离的报表  
对流入和流出的邮件归档可以实现远程存储  
强大的邮件监控、日志和报表  
失败、延迟和不能到达的邮件队列  
LDAP、RADIUS、POP3 和 IMAP 等多种 SMTP 认证方式  
基于每用户的动态白名单  
SNMP 标准库和私有库  
根据以下原则建立本地的发送者声誉列表：  
● 发送病毒的数量  
● 发送垃圾邮件的数量  
● 错误接收者的数量  
动态 DNS  
生成和发送 PDF 格式的报表  
灰色列表  
硬件平台  
支持多种语言  
正则表达式匹配  
DomainKeys  
DKIM  
分片邮件阻断  
虚拟机支持源和目标的 IP 地址池

## 拒绝式服务攻击

邮件炸弹  
接受地址的攻击  
邮件速率的限制  
反向 DNS 检测  
隐藏发件地址

## 加密

基于 ID 的加密  
S/MIME 支持网关到网关的加密  
支持 HTTPS、SMTPS、SSH、IMAPS 和 POP3S

## 高可用性

三种模式均支持  
A-P 模式  
邮件数据的同步  
会话级别的故障恢复  
设备失败检测和通知  
链路状态监控  
链路的故障恢复

## 日志和报表

快速向导式配置  
简单和高级两种配置模式  
实时统计  
多层管理员体系  
查找隔离能力  
定时生成 PDF 报告  
配置改变和管理事件记录  
防病毒事件日志  
反垃圾邮件事件日志  
支持外部和本地的 Syslog 服务器  
关键的事件和病毒报警  
140 多种 7 个大类的报表  
按时间规划生成报表  
字典模式触发归档

## 反垃圾——内容层的防御

流入和流出邮件过滤  
扩展的启发式垃圾邮件过滤  
附件和内容过滤  
深度邮件包头检测  
贝叶斯统计过滤  
SURBL  
禁忌词汇过滤  
流入和流出邮件过滤  
垃圾邮件隔离和邮件标记  
基于邮件的 SHASH 和黑名单技术的垃圾邮件管理(接受、中继、丢弃和抛弃)  
垃圾邮件图片扫描  
FortiGuard 反垃圾邮件服务  
全局和基于用户的黑白名单  
第三方实时黑名单  
伪造 IP 检测  
灰色列表检测

## 服务器模式的专有功能

POP3、SMTP 和 IMAP 邮件服务功能  
SMTP over SSL  
按用户的硬盘存储空间分配  
加密的 WebMail  
支持用户、组和别名  
本地帐户和 LDAP 认证  
垃圾邮件的专用文件夹

## 防病毒和反间谍软件

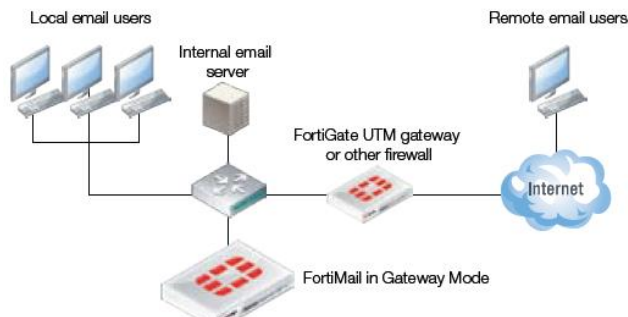
SMTP 邮件的病毒扫描  
支持压缩附件和多层嵌套  
隔离感染文件  
邮件的替代信息  
根据文件类型阻断  
附件过滤

# FortiMail 部署模式

用户可以根据自己网络实际情况来选择部署模式，透明、网关和服务器模式。

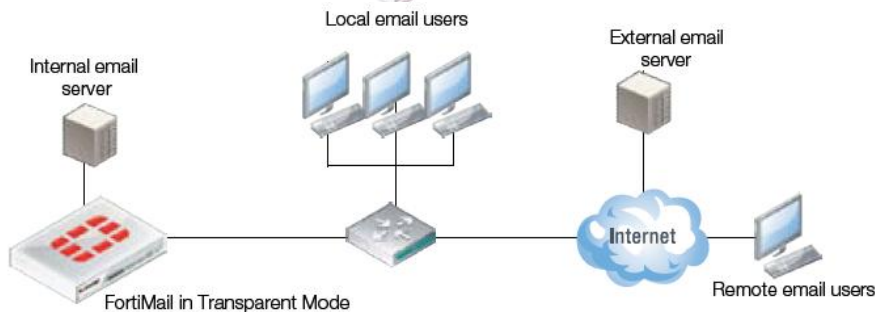
## 网关模式

可以对进出的所有邮件流量进行过滤。修改DNS的MX记录把邮件流量转向FortiMail。FortiMail接受邮件流量，对其进行病毒和垃圾邮件过滤，然后将干净的数据流转向邮件服务器。



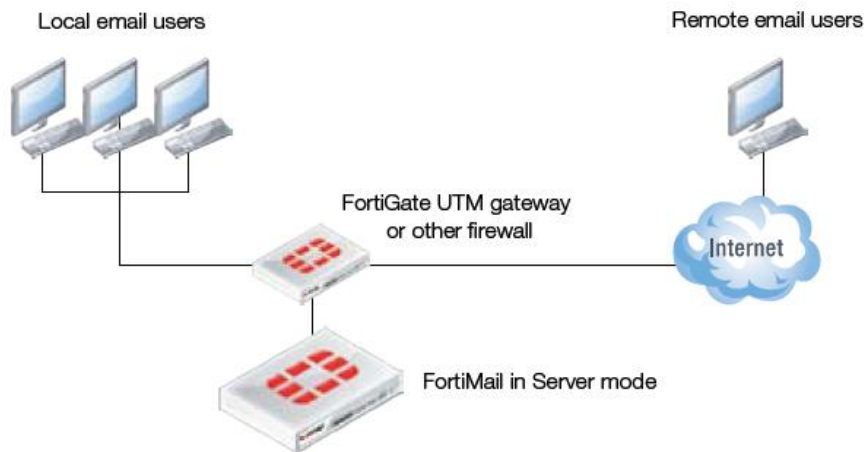
## 透明模式

FortiMail可以透明地部署于邮件服务器前，任何信息均不需要修改。FortiMail只需要在邮件流入的接口上启用邮件代理，即可对邮件进行过滤和扫描。该模式用户对网络的调整最小化，基本上不需要做任何改动。



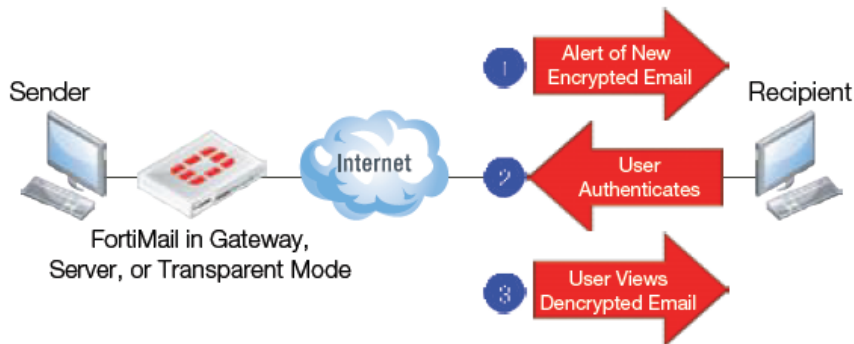
## 服务器模式

FortiMail可以作为独立邮件服务器，但是同时具有反垃圾邮件功能。它支持SMTP发送邮件，也支持POP3接受邮件，也可以支持IMAP和Web Mail。FortiMail在接受邮件和发送邮件时均进行病毒、垃圾邮件等过滤。



## 支持 IBE

IBE保证发送和接受机密邮件的安全可靠。部署IBE不需要额外的硬件、软件、不限用户或者其他许可费用。采用IBE技术可以减少纸面沟通和降低费用。FortiMail无论是透明模式、路由模式还是网关模式，均可以支持IBE。



### · 基于策略的加密方式

自动地对符合条件的邮件进行加密，无论是内容还是接收信息，均进行加密。

### · 推和拉的两种模式

无论采用推送还是拉送，或者混合模式，均可以满足要求。

### · 易于部署使用和管理:

部署IBE不需要增加任何费用，无论软件还是硬件的。

技术参数	FortiMail-100C	Fortimail-400B	FortiMail-2000B	FortiMail3000C	FortMail-5002B
<b>硬件指标</b>					
10/100 接口 (铜, RJ-45)	1	0	0	0	0
10/100/1000接口(铜, RJ-45)	2	4	6	4	3
SFP千兆接口	0	0	0	2	0
背板交换通道接口	0	0	0	0	2 / 2
扩展插槽	0	0	0	0	0
冗余电源	否	否	是	是	N/A
存储	1 TB	1x500 GB (1 TB 可选)	2x1 TB (6 TB 可选)	2x1 TB (6 TB 可选)	1x 146GB HDD (RTM)
<b>RAID</b>		软件	硬件	硬件	
	否	0, 1 (Raid 1 Requires	1, 5, 10, 50, Hot Spare	1, 5, 10, 50, Hot Spare	否
<b>系统参数</b>					
邮件域	50	500	5,000	5,000	10,000
基于接收者的策略 (虚拟域/系统)	60 / 300	600 / 3000	1,500 / 7,500	1,500 / 7,500	1,500 / 7,500
服务器模式邮箱数	200	1,000	3,000	3,000	3,000
防垃圾邮件、防病毒、内容监测的保护内容表 (虚拟域/系统)	50 / 60	50 / 200	50 / 600	50 / 600	50 / 600
不限用户数	Yes	Yes	Yes	Yes	Yes
<b>性能(3KB邮件, 无队列)</b>					
Email路由	90,000	300,000	1.5 Million	2.0 Million	2.3 Million
FortiGuard反垃圾邮件	85,000	280,000	1.3 Million	1.8 Million	2.2 Million
FortiGuard反垃圾邮件和防病毒	80,000	250,000	1.2 Million	1.6 Million	2.0 Million
<b>外形尺寸</b>					
HeightxWidthxLength (cm)	4.4x38x16 cm	4.5x43.8x36.8 cm	8.6x44.3x68.1 cm	8.6x44.3x68.1 cm	3 cmx32 x38 cm
weight	4 lbs (1.8 kg)	0 lb (4.5 kg)	57.5 lb (26.1 kg)	57.5 lb (26.1 kg)	5.9 lb (2.68 kg)
<b>环境要求</b>					
电源	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)
平均功率	56 W	121 W	152 W	200 W	148 W
散热	190.4 BTU	304 BTU	519 BTU	868 BTU	610 BTU
工作温度	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)
存储温度	-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)
湿度	5 to 95%非凝结	5 to 95%非凝结	5 to 95%非凝结	5 to 95%非凝结	5 to 93%非凝结
法规	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	FCC Class A, UL/CB/CUL, C Tick, VCCI, US EPA Energy Star	FCC Class A Part 15, UL/ CB/CUL
认证	VBSpam Platinum, Common Criteria EAL 2+, FIPS 140-2 Validation				FCC 47 CFR Part15, Class A, CE,UL60950-1/CSAC22.2

FortiMail 虚拟机	FortiMail-VM01	FortiMail-VM02
<b>技术参数</b>		
支持的虚拟机	VMware ESXi/ESX/4.0/4.1	VMware ESXi/ESX/4.0/4.1
最大支持 vCPUs	1	2
最大支持的虚拟网卡	4	4
虚拟存储 (最小 / 最大)	50 GB / 1 TB	50 GB / 1 TB
虚拟内存(最小/最大)	1 GB / 2 GB	1 GB / 4 GB
<b>性能(3KB邮件, 无队列)</b>		
Email路由	90,000	265,000
FortiGuard反垃圾邮件	85,000	234,000
FortiGuard反垃圾邮件和防病毒	77,000	185,400

FortiMail 虚拟机	FortiMail-VM01	FortiMail-VM02
<b>系统参数</b>		
邮件域	50	500
基于接收者的策略 (虚拟域/系统)	60 / 300	600 / 3000
服务器模式邮箱数	200	1000
防垃圾邮件、防病毒、内容监测的保护内容表 (虚拟域/系统)	50 / 60	50 / 200
不限用户数	Yes	Yes

飞塔信息科技（北京）有限公司  
地址: 北京市海淀区北四环西路52号中芯大厦12层 邮编: 100080  
电话: (010) 62960376  
传真: (010) 62960239  
售后: support\_cn@fortinet.com

飞塔信息科技（北京）有限公司海分公司  
地址: 上海市黄浦区南京西路338号天安中心1404室 邮编: 200021  
电话: (021) 6120 2836  
传真: (021) 6120 2856  
http://www.fortinet.com.cn

飞塔信息科技（北京）有限公司  
广州销售办公室  
广州市天河区体育西路101号维多利广场B塔1205室 邮编: 510620  
电话: (020) 2885 8303  
传真: (020) 2885 8378

**GLOBAL HEADQUARTERS**  
Fortinet Incorporated  
1090 Kifer Road, Sunnyvale,  
CA 94086 USA  
Tel: +1-408-235-7700  
Fax: +1-408-235-7737