FICHE PRODUIT

FortiMail™

FortiMail 200F, 400F, 900F, 2000E, 3000E, 3200E et machines virtuelles

FortiMail, passerelle de messagerie sécurisée de pointe, bloque les attaques ciblées et les attaques de masses. Elle sécurise la surface d'attaque dynamique de votre entreprise, prévient les pertes de données sensibles et vous aide à vous conformer aux réglementations. Les appliances physiques et virtuelles hautes performances se déploient localement ou via le cloud public pour accompagner les entreprises de toutes tailles, des PME aux grandes entreprises en passant par les opérateurs et prestataires de services.

Prévention contre les menaces

Notre solution anti-spam et anti-malware repose sur plusieurs technologies de pointe : protection instantanée contre les nouvelles attaques, désarmement et reconstitution des contenus, analyse par sandboxing, détection des usurpations d'identité, etc. Elle vous permet de stopper les spams, les logiciels rançonneurs (ransomwares), les attaques de messagerie et les cyberattaques ciblées.

Protection des données

Prévention efficace contre les pertes de données, chiffrement des e-mails (sur la base des identités) et archivage. Vous évitez la fuite accidentelle d'informations sensibles et vous conformez aux diverses réglementations professionnelles et sectorielles.

Écosystème Security Fabric

Compatibilité avec les produits Fortinet et les composants de la Security Fabric. Optez pour une cybersécurité proactive, via le partage des indicateurs de compromission au sein d'un système intégré baptisé Security Fabric.

Modes de déploiement

Passerelles de messagerie
Transparent
Serveur de messagerie complet

Assistance FortiCare 24h/24,7j/7 dans le monde entier

support.fortinet.com

Services de sécurité FortiGuard

www.fortiguard.com

Certifications indépendantes

Fonctionnalités

Anti-spam multi-niveaux

Inspection de l'expéditeur, du protocole, des contenus, ... : plus d'une douzaine de techniques protègent vos réseaux et utilisateurs contre les e-mails indésirables. Le filtrage débute notamment par l'évaluation de l'adresse IP et du domaine. Il se poursuit par le recours à d'autres outils évaluant la réputation de l'expéditeur, puis par diverses méthodes de validation telles que le rebond, l'authentification et la vérification du destinataire, les contrôles DMARC, DKIM et SPF. Enfin, la structure et le contenu des messages sont analysés à partir de la signature numérique, des mots-clés en contexte, de l'analyse des images, des URI embarquées et de techniques avancées (analyse comportementale, protection anti-spams). Utilisées conjointement, ces techniques permettent d'identifier et de bloquer 99,98 % des spams en conditions réelles.

Protection intégrée des données

Fonctionnalités de prévention des pertes de données, de chiffrement et d'archivage des e-mails. Protection des e-mails sensibles contre la parte accidentelle de données. Ces fonctionnalités aident au respect des réglementations (politiques de l'entreprises, réglementations sectorielles).

Gestion intuitive des e-mails

Tableaux de bord en temps réel, rapports complets, mises en quarantaine centralisées, fonction Mail Transfer Agent (MTA), fonctionnalités de traitement des e-mails... L'entreprise dispose d'une visibilité accrue et d'un contrôle maximum sur le trafic e-mails.

Déploiement flexible et performant

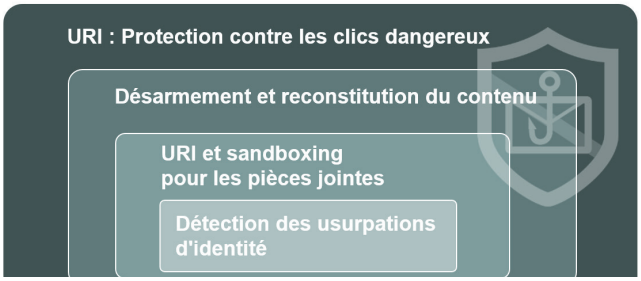
Déploiement évolutif permettant de traiter plus d'1,5 M de messages par heure (filtrage anti-spam et anti-malware complet). FortiMail s'adresse aux entreprises de toutes tailles. Il peut être déployé en mode passerelle, transparent ou serveur.

Anti-malware de pointe

FortiMail vous protège contre les cybermenaces en constante évolution. Son anti-malware associe plusieurs technologies statiques et dynamiques : analyses des signatures, analyses heuristiques, analyses comportementales et, en option, prévention contre les épidémies de virus.

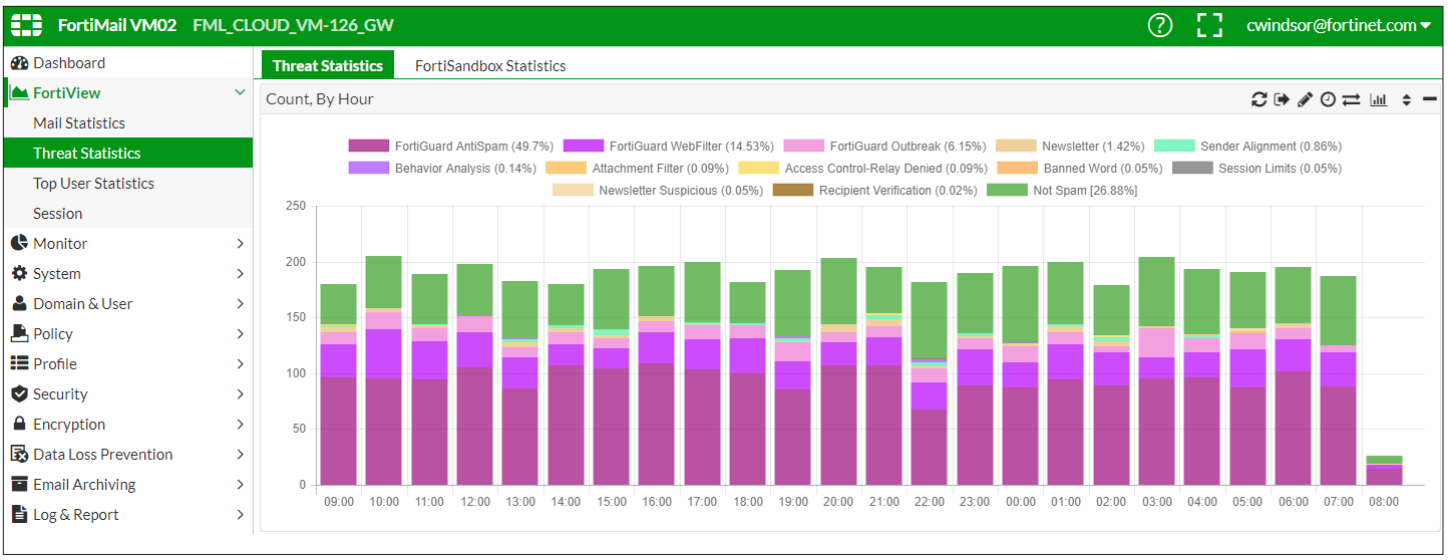
Protection avancée contre les menaces

Pour une défense encore plus efficace contre les menaces les plus récentes (attaques ciblées, attaques visant la messagerie), FortiMail propose en option le désarmement et la reconstitution des contenus, l'analyse sandboxing, la détection sophistiquée des usurpations d'identité et bien plus encore.



Intégration API

En s'appuyant sur les API de Microsoft Office 365 dans Exchange Online, FortiMail est capable de protéger efficacement le messagerie interne ainsi que les boîtes de réception des utilisateurs contre les menaces les plus récentes.



Déploiement

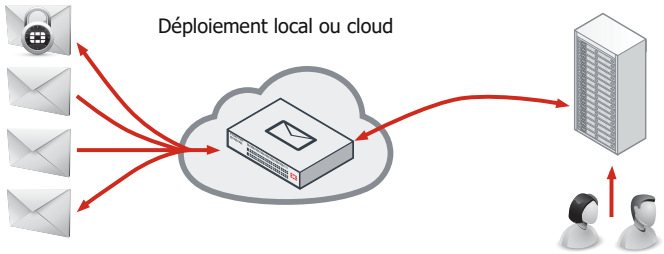
Plusieurs modes de déploiement - Transparent, Passerelle, Serveur et la nouvelle intégration API Office 365.

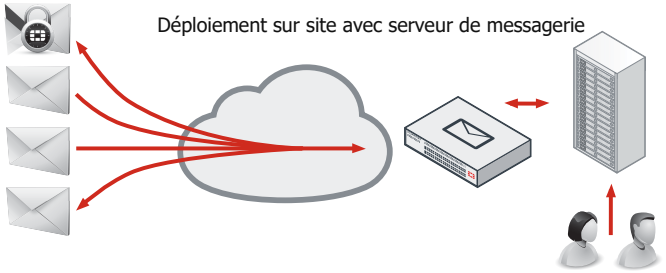
Mode passerelle : Ce mode fournit des services d'agent de transfert du courrier entrant et sortant par procuration (MTA) pour les passerelles de courrier électronique existantes. Un simple changement d'enregistrement DNS MX redirige les e-mails vers FortiMail pour une analyse anti-spam et anti-virus. FortiMail reçoit les messages, recherche les virus et les spams, puis transmet les e-mails à son serveur de messagerie de destination pour livraison.

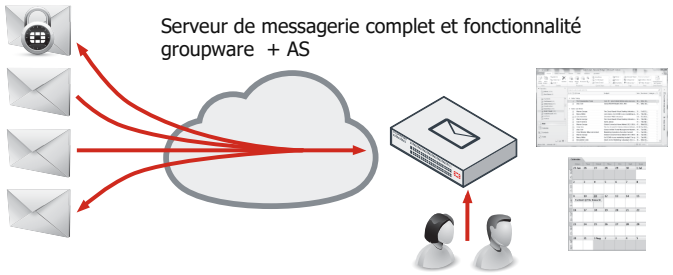
Mode transparent : Chaque interface réseau comprend un proxy qui reçoit et relaie les e-mails. Chaque proxy peut intercepter des sessions SMTP, même si l'adresse IP de destination n'est pas l'appliance FortiMail. FortiMail recherche les virus et les spams, puis transmet les e-mails au serveur de messagerie de destination pour livraison. Il n'est donc plus nécessaire de modifier l'enregistrement DNS MX ou de modifier la configuration réseau du serveur de messagerie existant.

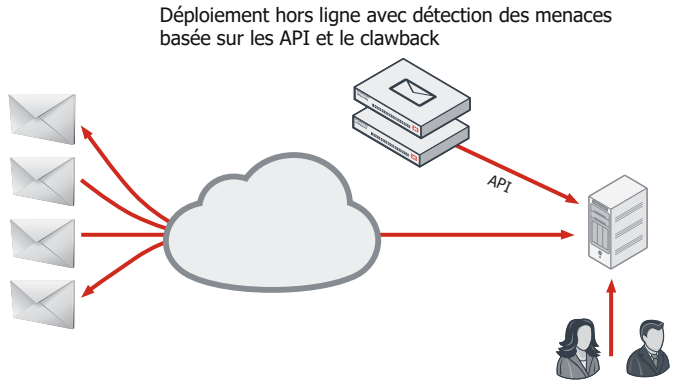
Mode serveur : Le dispositif FortiMail agit comme serveur de messagerie autonome avec toutes les fonctionnalités d'un serveur de messagerie SMTP, notamment la prise en charge flexible des accès sécurisés POP3, IMAP et WebMail. FortiMail analyse les e-mails pour détecter les virus et les spams avant livraison. Les MTA externes se connectent à FortiMail, pour lui permettre de fonctionner comme un serveur protégé.

Intégration API Office 365 : FortiMail peut être déployé hors ligne pour qu'aucun changement d'enregistrement MX ne soit nécessaire. FortiMail s'appuie sur l'API native de Microsoft Office 365 pour assurer la détection des menaces et la restitution (clawback) des messages après livraison. Ce fonctionnement présente une grande flexibilité : il est possible de créer des politiques répondant aux exigences de conformité ou aux besoins commerciaux uniques de chaque entreprise (création de paramètres de recherche basés sur des mots clés, sur les noms de fichier ou les types de contenus). Ces fonctionnalités viennent renforcer les fonctions de sécurité natives de Microsoft et maximisent les performances globales tout en réduisant les risques. D'autres améliorations à venir de l'intégration par API viendront apporter des fonctionnalités avancées d'analyse en temps réel et d'analyse des boîtes de réception internes.









Fonctionnalités

SYSTÈME

Large choix de déploiements :
- Mode transparent, passerelle et serveur
- Déploiement local ou cloud public/privé
- Service de gestion cloud

Inspection entrée et sortie

Prise en charge de plusieurs domaines de messagerie avec personnalisation par domaine :
- Prise en charge MSSP multilocataires, avec assistance en marque blanche
- Administration à plusieurs niveaux

Prise en charge des adresses IPv4 et IPv6

Hébergement virtuel utilisant des pools d'adresses IP source et/ou destination

Prise en charge de l'authentification SMTP via LDAP, RADIUS, POP3 et IMAP

Routage des e-mails LDAP

Inspection réalisée sur la base des attributs LDAP (fonctions des politiques de fonctionnement)

Interface webmail globale adaptée aux déploiements en mode serveur et à la gestion de la quarantaine

Gestion des files d'attente des e-mails

Prise en charge en plusieurs langues (webmail, interface d'administration)

Conformité SMTP RFC

Interface graphique HTML 5 moderne

Validé par des tests indépendants : VBSpam, NSS, ICSA

Compatibilité avec de nombreux services cloud comme Office365 et Google G-Suite

ANTISPAM

Service anti-spams FortiGuard
- Réputation de l'expéditeur et du domaine
- Signatures de pièces jointes et spams
- Règles heuristiques dynamiques
- Protection contre les épidémies

Le filtrage complet des catégories d'URL de FortiGuard comprend :
- Les URL de phishing, spams et logiciels malveillants
- Les URL pornographiques et réservés aux adultes
- Les domaines nouvellement enregistrés

Liste grise pour les adresses IPv4 et IPv6 et les comptes e-mails.

Réputation de l'expéditeur local (IPv4, IPv6 et ID Endpoint)

Analyse comportementale

Intégration en temps réel avec les URI de spam de tiers et les listes noires (SURBL/RBL)

Détection des newsletters (e-mails « gris ») et newsletters suspectes

Analyses PDF et analyses des images

Listes noires/blanches à plusieurs niveaux : global, domaine et utilisateur

Prise en charge des normes d'identité des expéditeurs d'entreprise :
- Sender Policy Framework (SPF)
- Domain Keys Identified Mail (DKIM)
- Domain-Based Message Authentication (DMARC)

Profils d'action et de notification flexibles

Quarantaines multi-systèmes et libre-service pour chaque utilisateur

PROTECTION CONTRE LES CYBERATTAQUES CIBLÉES

Désarmement et neutralisation des contenus :
- Neutralisation des documents Office et PDF (suppression des macros, des contenus actifs, des pièces jointes, etc.)
- Neutralisation des contenus HTML des e-mails en supprimant les hyperliens / en réécrivant les URL

Business Email Compromise (BEC):
- Protection anti-spoof multi-niveaux
- Analyse des usurpations d'identité - Détection manuelle et automatique des vols d'adresse
- Détection des domaines cousins

URL Click Protect réécrit les URL et les réanalyse lors de l'accès

Intégration à la plateforme FortiIsolator Browser Isolation pour neutraliser les menaces ciblant les navigateurs

INTÉGRATION API

Intégration Office 365 :
- Clawback des menaces après livraison
- Analyses programmées
- Analyse en temps réel
- Analyse du courrier interne

ANTIVIRUS

Détections anti-virus FortiGuard :
- Vérification des signatures de la CPRL
- Détections comportementales heuristiques
- Détection des logiciels indésirables

Protection FortiGuard Virus Outbreak :
- Renseignements sur les menaces collectés à l'échelle mondiale et analyse des données

Détection du contenu actif (PDF et documents Office)

Répétition du scan après libération de la quarantaine

Vérification du hachage des fichiers personnalisés

DÉTECTION DES CONTENUS

Détection mime + type de fichier

Prévention complète des pertes de données : prise d'empreintes des fichiers et détection des données sensibles
- Partage automatique de fichiers Windows et téléchargement manuel des empreintes de fichiers
- Détection des données personnelles, sanitaires et financières

Déchiffrement automatique des archives, des PDF et des documents Office à l'aide de listes de mots de passe intégrées et définies par l'administrateur. Détection de mots dans le corps des e-mails.

Analyse des images et des PDF

Service d'analyse dynamique d'images pour adultes :
- Identifie, signale ou bloque la transmission de contenus pour adultes

CHIFFREMENT

Prise en charge complète du chiffrement :
- TLS Serveur à serveur avec contrôle du chiffrement granulaire et exécution optionnelle
- S/MIME
- Chiffrement sans client vers le bureau du destinataire grâce au chiffrement basé sur l'identité (IBE)
- Plugin Outlook optionnel pour déclencher le chiffrement basé sur l'identité (IBE)

GESTION, JOURNAUX ET RAPPORTS

Modes de gestion de base/avancée

Comptes administrateurs en fonction du domaine et des attributions

Activité globale, modification des configurations, journaux et reporting des cyber incidents

Module de reporting intégré

Suivi détaillé des messages

Quarantaine centralisée pour les déploiements à grande échelle

Enregistrement et reporting centralisés en option avec FortiAnalyzer

Prise en charge SNMP via MIB standard et privés

Prise en charge des serveurs de stockage locaux ou externes, périphériques iSCSI y compris

Prise en charge Syslog externe

API Open REST pour la configuration et la gestion

HAUTE DISPONIBILITÉ (HA)

Haute disponibilité pour tous les scénarios de déploiement :
- Mode actif-passif
- Mode de synchronisation de la configuration actif-actif

Synchronisation de la quarantaine et de la file d'attente de messagerie

Détection et notification des pannes

Interfaces redondantes, failover, état de la liaison

FONCTIONNALITÉS AVANCÉES

Archivage du courrier électronique basé sur des règles avec options de stockage à distance : - Prise en charge de l'archivage des journaux Exchange

Prévention des pertes de données : prise d'empreintes des fichiers et à la détection des données sensibles
- CIFS automatique et transfert manuel des empreintes.
- Détection des renseignements personnels et informations importantes (santé, finances)

Fonctionnalités avancées du serveur de messagerie :
- Interface complète de messagerie web
- Accès au courrier POP3, IMAP
- Fonctions de calendrier
- Annuler l'envoi

Intégration SAML 2.0 SSO et ADFS pour le webmail et l'accès en quarantaine

ASSISTANCE

Options d'assistance simples inclues dans certains forfaits

Assistance RMA avancée

Services professionnels et options d'assistance à l'installation

Spécifications

			
	FORTIMAIL 200F	FORTIMAIL 400F	FORTIMAIL 900F
Scénarios de déploiement recommandés			
	Petites entreprises, succursales	Petites et moyennes entreprises	Moyennes et grandes entreprises, secteur de l'éducation, services gouvernementaux
Spécifications hardware			
Interfaces 10/100/1000 (cuivre, RJ45)	4	4	4
Interface Gigabit Ethernet SFP	0	0	2
Interface SFP+ 10 Gigabit Ethernet	0	0	0
Alimentations redondantes remplaçables à chaud	Non	Non	Oui
Stockage	1x 1To	2x 1To	2x 2To (2x 2To en option)
Gestion du stockage RAID	Non	Logiciel : 0, 1	Matériel : 1, 5, 10, Remplacement à chaud (En fonction du nombre de disques)
Format	1U	1U	1U
Alimentation électrique	Simple	Simple (Dual en option)	Dual
Spécifications système			
Domaines configurés*	20	100	800
Règles applicables en fonction du destinataire (par domaine / par système) - Entrant ou sortant	60 / 300	400 / 1 500	800 / 3 000
Boîtes aux lettres en mode serveur	150	400	1 500
Anti-spams, anti-virus, authentification et profils de contenu (par domaine / par système)	50 / 60	50 /200	50 / 400
Prévention des pertes de données	Non	Oui	Oui
Quarantaine centralisée	Non	Oui	Oui
Intégration API Office 365	Non	En option	En option
Performances (messages/heure) [Sans file d'attente pour des messages de 100 Ko]			
Routage e-mails (par heure)**	50 K	250 K	800 K
FortiGuard Antispam + Virus Outbreak (par heure)**	40 K	200 K	500 K
FortiGuard Enterprise ATP (par heure)**	30 K	150 K	400 K
Dimensions			
Hauteur x Largeur x Longueur (pouces)	1,73 x 17,24 x 16,61	1,73 x 17,24 x 16,38	1,75 x 17,00 x 27,61
Hauteur x Largeur x Longueur (mm)	44 x 438 x 422	44 x 438 x 416	44 x 438 x 701
Poids de l'appareil	5,4 kg (11,9 lbs)	11,0 kg (25,0 lbs)	15,00 kg (33,1 lbs)
Environnement			
Source d'alimentation	100–240V AC, 50–60 Hz	100–240V AC, 50–60 Hz	100–240V AC, 50–60 Hz
Courant maximal	100V / 3A, 240V / 1,5A	100V / 5A, 240V / 3A	100V / 5A, 240V / 2,5A
Puissance maximale requise	62 W	113 W	190 W
Consommation électrique (moyenne)	51 W	77 W	174 W
Dissipation de la chaleur	245 BTU/h	418 BTU/h	681 BTU/h
Humidité	5–90% sans condensation	5–90% sans condensation	5–90% sans condensation
Température de fonctionnement	0–40°C (32–104°F)	0–40°C (32–104°F)	0–40°C (32–104°F)
Température de stockage	-20–70°C (-4–158°F)	-20–70°C (-4–158°F)	-20–70°C (-4–158°F)
Conformité			
	FCC Partie 15 Classe A, C-Tick, VCCI, CE, UL/cUL, CB, RoHS	FCC Partie 15 Classe A, C-Tick, VCCI, CE, UL/cUL, CB, BSMI, RoHS	FCC Partie 15 Classe A, C-Tick, VCCI, CE, UL/cUL, CB, BSMI, RoHS
Certifications			
	VBSpam et VB100, Common Criteria NDPP, Certifié FIPS 140-2	VBSpam et VB100, Common Criteria NDPP, Certifié FIPS 140-2	VBSpam et VB100, Common Criteria NDPP, Certifié FIPS 140-2

* Les domaines configurés correspondent au nombre total de domaines de messagerie pouvant être configurés sur l'appliance. Les associations de domaines peuvent être utilisées pour activer des domaines secondaires partageant la configuration du domaine principal.
** Testé avec FortiMail 6.0

Spécifications



	FORTIMAIL 2000E	FORTIMAIL 3000E	FORTIMAIL 3200E
Scénarios de déploiement recommandés			
	Grandes entreprises, éducation et institutions gouvernementales	L'appliance la plus performante pour les structures les plus importantes : universités, entreprises, FAI et opérateurs.	
Spécifications hardware			
Interfaces 10/100/1000 (cuivre, RJ45)	4	4	4
Interface Gigabit Ethernet SFP	2	2	2
Interface SFP+ 10 Gigabit Ethernet	0	0	2
Alimentations redondantes remplaçables à chaud	Oui	Oui	Oui
Stockage	2x 2 To (10x 2 To Optionnel)	2x 2 To SAS (10x 2 To Optionnel)	2x 2 To (10x 2 To Optionnel)
Gestion du stockage RAID	Matériel : 1, 5, 10, Remplacement à chaud (En fonction du nombre de disques)	Matériel : 1, 5, 10, Remplacement à chaud (En fonction du nombre de disques)	Matériel : 1, 5, 10, Remplacement à chaud (En fonction du nombre de disques)
Format	2U	2U	2U
Alimentation électrique	Dual	Dual	Dual
Spécifications système			
Domaines configurés*	800	2 000	2 000
Règles applicables en fonction du destinataire (par domaine / par système) - Entrant ou sortant	800 / 3 000	1 500 / 7 500	1 500 / 7 500
Boîtes aux lettres en mode serveur	2 000	3 000	3 000
Anti-spams, anti-virus, authentification et profils de contenu (par domaine / par système)	50 / 400	50 / 600	50 / 600
Prévention des pertes de données	Oui	Oui	Oui
Quarantaine centralisée	Oui	Oui	Oui
Intégration API Office 365	Optionnel	Optionnel	Optionnel
Performances (messages/heure) [Sans file d'attente pour des messages de 100 Ko]			
Routage e-mails (par heure)**	1,5 million	2,5 millions	3,4 millions
FortiGuard Antispam + Virus Outbreak (par heure)**	1,0 million	1,8 million	2,4 millions
FortiGuard Enterprise ATP (par heure)**	700 000	1,5 million	2,0 millions
Dimensions			
Hauteur x Largeur x Longueur (pouces)	3,5 x 17,2 x 25,5	3,5 x 17,2 x 25,5	3,5 x 17,2 x 25,5
Hauteur x Largeur x Longueur (mm)	89 x 437 x 647	89 x 437 x 647	89 x 437 x 647
Poids de l'appareil	14,5 kg (32 lbs)	18,2 kg (40.0 lbs)	18,2 kg (40.0 lbs)
Environnement			
Source d'alimentation	100–240V AC, 50–60 Hz	100–240V AC, 50–60 Hz	100–240V AC, 50–60 Hz
Courant maximal	10,0A /110V, 3,5A /240V	9,8A / 110V, 4,9A / 220V	9,8A / 110V, 4,9A / 220V
Puissance maximale requise	219 W	379 W	382 W
Consommation électrique (moyenne)	189 W	348 W	351 W
Dissipation de la chaleur	781 BTU/h	1325 BTU/h	1336 BTU/h
Humidité	8–90% sans condensation	8–90% sans condensation	8–90% sans condensation
Température de fonctionnement	41–95°F (5–35°C)	50–95°F (10–35°C)	50–95°F (10–35°C)
Température de stockage	-40–140°F (-40–60°C)	-40–158°F (-40–70°C)	-40–158°F (-40–70°C)
Conformité			
	FCC Partie 15 Classe A, C-Tick, VCCI, CE, UL/cUL, CB, BSMI, RoHS	FCC Partie 15 Classe A, C-Tick, VCCI, CE, UL/cUL, CB, BSMI, RoHS	FCC Partie 15 Classe A, C-Tick, VCCI, CE, UL/cUL, CB, BSMI, RoHS
Certifications			
	VBSpam et VB100, Common Criteria NDPP, Certifié FIPS 140-2	VBSpam et VB100, Common Criteria NDPP, Certifié FIPS 140-2	VBSpam et VB100, Common Criteria NDPP, Certifié FIPS 140-2

* Les domaines configurés correspondent au nombre total de domaines de messagerie pouvant être configurés sur l'appliance. Les associations de domaines peuvent être utilisées pour activer des domaines secondaires partageant la configuration du domaine principal.
** Testé avec FortiMail 6.0

Spécifications

SPÉCIFICATIONS TECHNIQUES POUR LES APPLIANCES VIRTUELLES FORTIMAIL	VM00	VM01	VM02	VM04	VM08	VM16	VM32
Scénarios de déploiement recommandés							
	Demonstrations, tests, formations	Petites organisations, succursales	Petites et moyennes organisations	Moyennes à grandes entreprises	Grandes entreprises	Grandes entreprises	Grandes entreprises
Spécifications techniques							
Hyperviseurs pris en charge	VMware ESXi 5.0/5.1/5.5/6.0/6.5, Citrix / OpenSource XenServer 5.6 SP2/6.0 et ultérieur Microsoft Hyper-V 2008 R2/2012/2012 R2/2016, KVM (qemu 0.12.1et ultérieur), AWS (Amazon Web Services), Microsoft Azure						
Nombre maximum de processeurs virtuels pris en charge	1	1	2	4	8	16	32
NIC virtuels requis (Minimum/Maximum)	1 / 4	1 / 4	1 / 4	1 / 6	1 / 6	1 / 6	1 / 6
Stockage requis pour la machine virtuelle (Minimum/Maximum)	50 GB / 1 TB	50 GB / 1 TB	50 GB / 2 TB	50 GB / 4 TB	50 GB / 8 TB	50 GB / 12 TB	50 GB / 24 TB
Mémoire requise pour la machine virtuelle (Minimum/Maximum)	2 GB / 2 GB	2 GB / 4 GB	2 GB / 8 GB	4 GB / 16 GB	4 GB / 64 GB	4 GB / 128 GB	4 GB / 128 GB
Performances (messages/heure) [Sans file d'attente pour des messages de 100 Ko]							
Routage e-mails	3,6 K	34 K	67 K	306 K	675 K	875 K	1,2 M
FortiGuard Anti-spam	3,1 K	30 K	54 K	279 K	630 K	817 K	1,1 M
FortiGuard Anti-spam + Anti-virus	2,7 K	26 K	52 K	225 K	585 K	758 K	1,0 M
Spécifications système							
Domaines configurés **	2	20	100	800	1 000	2 000	2 000
Règles basées sur les bénéficiaires (domaine/système) - Entrants ou sortants	15 /30	60 /300	400 / 1 500	800 / 3 000	800 / 3 000	1 500 / 7 500	1 500 / 7 500
Boîtes aux lettres en mode serveur	50	150	400	1 500	2 000	3 000	3 000
Anti-spams, anti-virus, authentification et profils de contenu (par domaine / par système)	10 / 15	50 / 60	50 / 200	50 / 400	50 / 400	50 / 600	50 / 600
Prévention des pertes de données	Non	Non	Oui	Oui	Oui	Oui	Oui
Quarantaine centralisé	Non	Non	Oui	Oui	Oui	Oui	Oui
Intégration API Office365	Non	Non	Optionnel	Optionnel	Optionnel	Optionnel	Optionnel

* Dépend du matériel. Chiffres indicatifs basés sur plusieurs machines virtuelles fonctionnant sur un système partagé.*
** Les domaines configurés correspondent au nombre total de domaines de messagerie pouvant être configurés sur l'appliance. Les associations de domaines peuvent être utilisées pour activer des domaines secondaires partageant la configuration de leur domaine principal.
*** Le déploiement en mode transparent n'est pas entièrement pris en charge par Microsoft HyperV et par les hyperviseurs cloud, compte-tenu des limitations relatives aux configurations réseau disponibles.

Informations relatives aux commandes

Produit	Référence/SKU	Description
FortiMail 200F	FML-200F	Email Security Appliance — 4 ports GE RJ45, 1 To de stockage
FortiMail 400F	FML-400F	Email Security Appliance — 4 ports GE RJ45, 2 To de stockage
FortiMail 900F	FML-900F	Email Security Appliance — 4 ports GE RJ45, 2 emplacements GE SFP, alimentation dual AC, 4 To de stockage par défaut.
FortiMail 2000E	FML-2000E	Email Security Appliance — 4 ports GE RJ45, 2 emplacements GE SFP, alimentation dual AC, 4 To de stockage par défaut.
FortiMail 3000E	FML-3000E	Email Security Appliance — 4 ports GE RJ45, 2 emplacements GE SFP, alimentation dual AC, 4 To de stockage par défaut.
FortiMail 3200E	FML-3200E	Email Security Appliance — 4 ports GE RJ45, 2x10 emplacements GE SFP+, 2 emplacements GE SFP, alimentation dual AC, 4 To de stockage par défaut.
FortiMail VM00	FML-VM00	Appliance virtuelle FortiMail-VM pour les plateformes de virtualisation VMware ESX/ESXi, Microsoft Hyper-V, Citrix XenServer et KVM. 1x noyau vCPU.
FortiMail VM01	FML-VM01	Appliance virtuelle FortiMail-VM pour les plateformes de virtualisation VMware ESX/ESXi, Microsoft Hyper-V, Citrix XenServer et KVM. 1x noyau vCPU.
FortiMail VM02	FML-VM02	Appliance virtuelle FortiMail-VM pour les plateformes de virtualisation VMware ESX/ESXi, Microsoft Hyper-V, Citrix XenServer et KVM. 2x cœurs vCPU.
FortiMail VM04	FML-VM04	Appliance virtuelle FortiMail-VM pour les plateformes de virtualisation VMware ESX/ESXi, Microsoft Hyper-V, Citrix XenServer et KVM. 4x cœurs vCPU.
FortiMail VM08	FML-VM08	Appliance virtuelle FortiMail-VM pour les plateformes de virtualisation VMware ESX/ESXi, Microsoft Hyper-V, Citrix XenServer et KVM. 8x cœurs vCPU.
FortiMail VM16	FML-VM16	Appliance virtuelle FortiMail-VM pour les plateformes de virtualisation VMware ESX/ESXi, Microsoft Hyper-V, Citrix XenServer et KVM. 16x cœurs vCPU.
FortiMail VM32	FML-VM32	Appliance virtuelle FortiMail-VM pour les plateformes de virtualisation VMware ESX/ESXi, Microsoft Hyper-V, Citrix XenServer et KVM. 32x cœurs vCPU.
FortiMail Cloud		
FortiMail Cloud — Serveur	FC-10-0VM01-416-02-DD	FortiMail Cloud — Serveur (25–100 boîtes de réception)
	FC-10-0VM01-417-02-DD	FortiMail Cloud — Serveur Premium (25–100 boîtes de réception)
FortiMail Cloud — Passerelle	FC-10-0VM01-414-02-DD	FortiMail Cloud — Passerelle (25–100 boîtes de réception)
	FC-10-0VM02-414-02-DD	FortiMail Cloud — Passerelle (101–1 000 boîtes de réception)
	FC-10-0VM04-414-02-DD	FortiMail Cloud — Passerelle (1 001–5 000 boîtes de réception)
	FC-10-0VM08-414-02-DD	FortiMail Cloud — Passerelle (5 001–10 000 boîtes de réception)
	FC-10-0VM16-414-02-DD	FortiMail Cloud — Passerelle (10 000+ boîtes de réception)
	FC-10-0VM01-415-02-DD	FortiMail Cloud — Passerelle Premium (25–100 boîtes de réception)
	FC-10-0VM02-415-02-DD	FortiMail Cloud — Passerelle Premium (101–1 000 boîtes de réception)
	FC-10-0VM04-415-02-DD	FortiMail Cloud — Passerelle Premium (1 001–5 000 boîtes de réception)
	FC-10-0VM08-415-02-DD	FortiMail Cloud — Passerelle Premium (5 001–10 000 boîtes de réception)
	FC-10-0VM16-415-02-DD	FortiMail Cloud — Passerelle Premium (10 000+ boîtes de réception)
FortiMail Cloud — Passerelle MSSP	FC1-10-EVMSP-415-02-DD	FortiMail Cloud — Passerelle Premium pour MSSP (500–1 000 boîtes de réception)
	FC2-10-EVMSP-415-02-DD	FortiMail Cloud — Passerelle Premium pour MSSP (1 001–10 000 boîtes de réception)
	FC3-10-EVMSP-415-02-DD	FortiMail Cloud — Passerelle Premium pour MSSP (10 000+ boîtes de réception)
FortiMail Cloud — Passerelle Premium avec Office365	FC-10-0VM02-423-02-DD	FortiMail Cloud — Passerelle Premium avec prise en charge API Office365 (100 à 1 000 boîtes de réception)
	FC-10-0VM04-423-02-DD	FortiMail Cloud — Passerelle Premium avec prise en charge API Office365 (1 001 à 5 000 boîtes de réception)
	FC-10-0VM08-423-02-DD	FortiMail Cloud — Passerelle Premium avec prise en charge API Office365 (5 001 à 10 000 boîtes de réception)
	FC-10-0VM16-423-02-DD	FortiMail Cloud — Passerelle Premium avec prise en charge API Office365 (10 000+ boîtes de réception)
FortiMail Cloud — FortiGuard Add-on d'analyse de contenus	FC-10-FMLC0-160-02-DD	Add-on d'analyse de contenus FortiGuard pour les services FortiMail Cloud (par boîte de réception)
Accessoires		
Bloc d'alimentation pour FML-400E	SP-FAD700-PS	Alimentation AC supplémentaire pour FML-400E.
Alimentation pour FML-2000E	SP-FML2000E-PS	Alimentation AC de remplacement pour FML-2000E.
Alimentation pour FML-3000E et FML-3200E	SP-FML3000E-PS	Alimentation de remplacement pour FML-3000E et FML-3200E.
HDD pour FML-3000E	SP-D2TE	Disque dur SAS 3,5" de 2 To avec plateau pour FML-2000E, FML-3000E et FML-3200E.
HDD pour FML-900F	SP-FML900F-HDD	Disque dur SAS 3,5" de 2 To avec plateau pour FML-900F
Alimentation pour FML-400F et FML-900F	SP-FML900F-PS	Alimentation de remplacement pour FML-400F et FML-900F

FORTINET®

www.fortinet.com