FortiMail Antispam : Configuration Complète 2026

> FortiMail est la passerelle email sécurisée de Fortinet : son moteur antispam multicouche combine FortiGuard DNSBL, analyse bayésienne, heuristique comportementale et vérification SPF/DKIM/DMARC. Ce guide couvre la configuration complète, du profil antispam de base au tuning avancé, pour les administrateurs qui déploient FortiMail en mode Gateway ou Server dans des environnements PME/ETI français.

La messagerie électronique reste le vecteur d'attaque numéro un en 2026 : 91 % des cyberattaques débutent par un email malveillant, et les campagnes de phishing ciblant les entreprises françaises ont progressé de 34 % en un an selon les données CERT-FR. Dans ce contexte, la configuration rigoureuse d'une passerelle antispam n'est plus optionnelle — c'est une mesure de sécurité de premier rang, au même titre qu'un pare-feu ou un EDR. FortiMail, la solution de messagerie sécurisée de Fortinet, propose une architecture antispam multicouche particulièrement complète : filtrage IP par réputation, analyse heuristique, moteur bayésien auto-apprenant, vérification des enregistrements DNS d'authentification email (SPF, DKIM, DMARC), et intégration avec le service cloud FortiGuard Antispam pour une protection en temps réel contre les nouvelles campagnes. Mais la puissance de FortiMail ne s'exprime pleinement qu'avec une configuration adaptée au contexte métier : un profil antispam trop agressif génère des faux positifs qui bloquent des emails légitimes, tandis qu'une configuration trop permissive laisse passer des malwares et du phishing. Ce guide technique détaillé vous accompagne étape par étape dans la configuration d'une protection antispam FortiMail optimale, depuis la mise en place des profils jusqu'au tuning avancé et à la configuration des rapports de quarantaine pour vos utilisateurs. Les exemples de commandes CLI couvrent FortiMail OS 7.x (dernière branche stable en 2026).

À RETENIR

⚡ À retenir — FortiMail Antispam

FortiMail combine 8 moteurs de filtrage indépendants : IP Reputation FortiGuard, DNSBL, analyse heuristique, bayésien auto-apprenant, vérification SPF/DKIM/DMARC, analyse de contenu et d'URL, et sandboxing FortiSandbox optionnel. La protection optimale nécessite d'activer les trois couches — réseau (IP reputation), protocole (SPF/DKIM/DMARC) et contenu (heuristique + bayésien) — et de déployer FortiMail en mode Gateway devant votre serveur Exchange ou Microsoft 365. Le tuning bayésien prend 2 à 4 semaines de formation pour atteindre son efficacité maximale.

Architecture antispam FortiMail : flux de traitement et moteurs

FortiMail traite chaque email entrant selon un pipeline séquentiel de filtrage. Comprendre ce pipeline est indispensable pour diagnostiquer les problèmes et optimiser la configuration. Le flux de traitement commence dès l'établissement de la connexion SMTP : avant même la réception du corps du message, FortiMail applique des filtres au niveau de la session TCP.

Le pipeline de traitement antispam FortiMail fonctionne dans cet ordre :

Filtrage IP (connexion) : vérification de l'IP source contre les listes noires locales, FortiGuard IP Reputation et les DNSBL configurées. Si l'IP est répertoriée, la connexion est rejetée avec un code 550 avant toute transmission de données.

Vérifications SMTP : validation du HELO/EHLO, vérification du domaine d'envoi (RDNS lookup), limitation du taux de connexion (rate limiting) par IP et par domaine.

Authentification email : vérification SPF sur l'enveloppe MAIL FROM, vérification DKIM sur les en-têtes, évaluation de la politique DMARC. Les résultats alimentent le score global.

Analyse de contenu : analyse heuristique du corps du message (patterns de spam connus, structure HTML suspecte, ratio image/texte), vérification des URLs contre FortiGuard Web Filter, analyse bayésienne.

Classification finale : agrégation des scores et application de l'action définie dans le profil antispam (délivrer, mettre en quarantaine, rejeter, taguer).

FortiMail peut opérer en trois modes : **Gateway** (MX record pointe vers FortiMail, qui relaie vers le serveur de messagerie interne), **Server** (FortiMail est lui-même le serveur de messagerie, avec boîtes aux lettres) et **Transparent** (déployé en ligne sans modification des enregistrements DNS, via bridge). Le mode Gateway est le plus courant pour les organisations qui conservent Exchange ou Microsoft 365 comme serveur de destination.

Modes de déploiement : Gateway, Server et Transparent

Le choix du mode de déploiement FortiMail conditionne l'ensemble de la configuration antispam et doit être arrêté avant toute autre paramétrage.

Mode Gateway : le MX record de votre domaine pointe vers FortiMail. Tous les emails entrants transitent par FortiMail, qui les filtre puis les relaie vers votre serveur de messagerie (Exchange, Postfix, Microsoft 365 via connecteur). C'est le mode recommandé pour la grande majorité des déploiements en entreprise. Il permet également de filtrer les emails sortants, réduisant le risque de voir votre domaine blacklisté suite à une compromission interne.

Mode Server : FortiMail héberge directement les boîtes aux lettres. Ce mode est utilisé lorsque l'organisation souhaite remplacer complètement son infrastructure de messagerie. Il offre les mêmes capacités antispam mais avec une gestion plus complexe (comptes, quotas, accès webmail).

Mode Transparent : FortiMail est inséré physiquement dans le flux réseau entre le pare-feu et le serveur de messagerie, sans modification des enregistrements DNS. Ce mode est utile pour un déploiement rapide ou des POC, mais limite certaines fonctionnalités (notamment la vérification DMARC complète sur les emails sortants).

Pour configurer le mode de déploiement : *System* > *Network* > *Operation Mode*. En CLI : `config system global; set operation-mode gateway; end`. Consultez le guide des modes opératoires GUI FortiMail pour la procédure détaillée de changement de mode.

Profils antispam FortiMail : création et paramétrage

Les profils antispam sont le cœur de la configuration FortiMail. Un profil antispam définit quels moteurs activer, comment agréger leurs scores, et quelle action appliquer selon la classification finale (spam, probable spam, propre). FortiMail permet de créer plusieurs profils et de les appliquer différemment selon le sens du flux (entrant/sortant), le domaine destinataire ou l'adresse source.

Pour créer un nouveau profil antispam : *Anti-Spam* > *Profiles* > *New*. Les paramètres fondamentaux d'un profil :

Spam Detection Action : action appliquée aux messages classifiés comme spam. Options : *Reject* (rejet SMTP 550, recommandé pour le spam certain), *Discard* (accepté puis supprimé silencieusement), *Tag* (ajout d'un préfixe dans le sujet, ex: [SPAM]), *Quarantine* (mise en attente pour révision).

Probable Spam Action : action pour les messages à score intermédiaire. La quarantaine est généralement préférable au rejet pour éviter les faux positifs.

Spam Threshold : seuil de score au-delà duquel un message est classifié comme spam. Valeur par défaut : 100. Un seuil plus bas augmente la détection mais aussi les faux positifs.

Probable Spam Threshold : seuil pour la classification "probable spam". Typiquement 50 à 80.

En CLI, la création d'un profil antispam s'effectue ainsi :

```
config antispam profile
  edit "profile-entrant-standard"
    set comment "Profil antispam pour flux entrant standard"
    set spam-bwl-check enable
    set spam-iwl-check enable
    set spam-dul-check enable
    set fortiguard-email-check enable
    set spam-hdrcheck enable
    set spam-bayesian-check enable
    set spam-rbl-check enable
    config spam-rbl-table
      edit 1
        set server "zen.spamhaus.org"
        set status enable
      next
    end
  next
end
```

Voir la référence CLI/SSH FortiMail complète pour toutes les options de configuration en ligne de commande.

FortiGuard Antispam Service : activation et configuration

Le service FortiGuard Antispam est le composant cloud de Fortinet qui fournit des mises à jour en temps réel des bases de données IP reputation, empreintes de spam et URLs malveillantes. Son activation est indispensable pour une protection efficace contre les nouvelles campagnes — les définitions locales seules sont insuffisantes face à l'évolution rapide des techniques des spammeurs.

Pour activer FortiGuard Antispam : *System* > *FortiGuard* > *AntiSpam*. FortiMail doit disposer d'une licence FortiGuard Antispam valide (distincte de la licence FortiGuard Web Filter). Vérifiez l'état de la licence dans *System* > *Dashboard* > *License Information*.

Les composants FortiGuard Antispam activables dans les profils :

FortiGuard Email Checksum : compare les empreintes MD5 des messages contre la base de signatures FortiGuard. Très efficace contre les campagnes en masse qui utilisent des templates identiques.

FortiGuard URI Check : vérifie les URLs présentes dans le message contre le service FortiGuard Web Filter. Détecte les liens vers des sites de phishing et malware.

FortiGuard Spam Submission : envoie les faux négatifs confirmés à Fortinet pour enrichir la base de données globale (opt-in, désactivé par défaut).

IP Black List (FortiGuard) : bloque les connexions SMTP provenant d'IPs répertoriées comme spammeurs actifs dans la base FortiGuard, avec mise à jour en temps réel.

La consultation des bases FortiGuard s'effectue en deux modes : *Push* (FortiGuard pousse les mises à jour vers FortiMail, latence nulle) ou *Pull* (FortiMail interroge FortiGuard périodiquement, moins recommandé). Configurez le mode Push dans *System* > *FortiGuard* > *Push Update*.

En CLI : `diagnose fortiguard-service status antispam` pour vérifier la connexion et la fraîcheur des bases.

Documentation officielle : FortiGuard Antispam — FortiMail 7.4 Admin Guide.

SPF, DKIM et DMARC dans FortiMail : vérification et actions

L'authentification email (SPF, DKIM, DMARC) est la première ligne de défense contre l'usurpation d'identité et le phishing. FortiMail intègre nativement la vérification de ces trois standards et permet de configurer des actions différenciées selon les résultats — de la simple annotation à la quarantaine ou au rejet.

Configuration SPF : dans le profil antispam, section *Authentication*, activez *Sender Policy Framework (SPF)*. Options d'action : *None* (annoter uniquement), *Quarantine* (mettre en quarantaine si SPF fail), *Reject* (rejeter si SPF fail avec code 550). La recommandation pour un environnement de production est de commencer par *None* pendant deux semaines pour mesurer

le volume de faux positifs, puis de passer à *Quarantine*, et enfin à *Reject* si le taux de faux positifs est acceptable.

Configuration DKIM : activez *DomainKeys Identified Mail (DKIM)* dans le profil antispam. FortiMail vérifie la signature DKIM du message contre la clé publique publiée dans le DNS de l'expéditeur. Un *DKIM fail* (signature invalide ou absente sur un domaine qui la requiert) est un signal fort de phishing ou de relais non autorisé.

Configuration DMARC : la vérification DMARC agrège les résultats SPF et DKIM et applique la politique publiée par le domaine expéditeur (none/quarantine/reject). Activez *Domain-based Message Authentication, Reporting, and Conformance (DMARC)* dans le profil. FortiMail respecte la politique DMARC déclarée par le domaine expéditeur — si ce domaine publie `p=reject`, FortiMail rejettera les messages qui échouent l'alignement DMARC, indépendamment du score spam global.

Pour votre propre domaine émetteur, consultez notre guide sur la configuration DMARC, DKIM et SPF complète — la configuration FortiMail émetteur (signature DKIM sortante, rapport DMARC) est complémentaire à la vérification entrante.

En CLI, activation des vérifications d'authentification :

```
config antispam profile
  edit "profile-entrant-standard"
    set spam-sender-check enable
    set sender-policy-check enable
    set sender-domain-policy-check enable
    set dkim-check enable
    set dmarc-check enable
    set dmarc-quarantine enable
    set dmarc-reject enable
  next
end
```

Listes blanches, listes noires et gestion des faux positifs

Aucun moteur antispam n'atteint une précision parfaite : les faux positifs (emails légitimes classifiés comme spam) et les faux négatifs (spam non détecté) sont inévitables. FortiMail propose plusieurs mécanismes pour gérer ces cas sans compromettre la sécurité globale.

Listes blanches d'expéditeurs (Sender White List) : les emails provenant d'expéditeurs ou de domaines inscrits sur la liste blanche contournent les moteurs antispam. À utiliser avec extrême parcimonie : une liste blanche trop généreuse est un vecteur d'attaque si un partenaire est compromis. Préférez inscrire des adresses email individuelles plutôt que des domaines entiers.

Configuration : *Anti-Spam > Black/White List > Sender White List > New*. Format : adresse email (`contact@fournisseur.fr`), pattern (`@fournisseur.fr`) ou plage IP (`203.0.113.0/24`).

Listes noires d'expéditeurs (Sender Black List) : les emails provenant d'expéditeurs inscrits sont automatiquement rejetés ou mis en quarantaine. Utile pour bloquer des sources de spam persistantes non répertoriées par FortiGuard.

Quarantaine utilisateur et self-service : FortiMail permet aux utilisateurs finaux de consulter leur quarantaine personnelle via un portail web et de libérer eux-mêmes les faux positifs, réduisant la charge sur les administrateurs. La configuration du portail de quarantaine : *Anti-Spam > Quarantine > User Quarantine > Settings*. Activez les rapports de quarantaine journaliers par email : *Schedule Report > Enable*, fréquence *Daily*, heure *08:00*. Les utilisateurs reçoivent chaque matin un récapitulatif des messages en quarantaine avec des liens de libération à usage unique.

Formation bayésienne par les utilisateurs : si vous activez le moteur bayésien (recommandé), vous pouvez permettre aux utilisateurs de signaler des faux positifs/négatifs via le portail quarantaine. Ces signalements enrichissent le modèle bayésien local, améliorant la précision au fil du temps. Pour ce faire : *Anti-Spam > Bayesian > Bayesian DB > Enable User Submission*.

Quarantaine : configuration, gestion et rapports

La quarantaine FortiMail est un espace de stockage intermédiaire où les messages suspects sont conservés avant une décision définitive (livraison ou suppression). Elle est distincte de la suppression immédiate et offre un filet de sécurité contre les faux positifs — un message mis en quarantaine peut toujours être récupéré, contrairement à un message rejeté ou supprimé.

FortiMail propose deux types de quarantaine :

Quarantaine système : accessible uniquement aux administrateurs. Reçoit les messages classifiés comme spam certain. Les administrateurs peuvent rechercher, prévisualiser et libérer des messages depuis *Anti-Spam > Quarantine > System Quarantine*.

Quarantaine utilisateur : accessible à l'utilisateur final via un portail web. Reçoit les messages classifiés comme probable spam. L'utilisateur peut les libérer sans intervention de l'administrateur.

Configuration de la quarantaine système :

```
config antispam quarantine
  set max-msgs 100000
  set max-msg-size 10
  set quota-warning-level 80
  set expire-time 14
  set report-send enable
  set report-interval daily
  set report-format text
end
```

Le paramètre `expire-time 14` conserve les messages en quarantaine pendant 14 jours avant suppression automatique — ajustez selon vos obligations de rétention et l'espace disque disponible. Le quota `quota-warning-level 80` génère une alerte admin quand la quarantaine atteint 80 % de sa capacité.

Pour la quarantaine utilisateur et le portail self-service, assurez-vous que le FQDN du portail FortiMail est accessible depuis le réseau des utilisateurs. Le port par défaut du portail quarantaine est 443 (HTTPS). Configurez un certificat TLS valide pour éviter les avertissements navigateur.

Tuning avancé : bayésien, heuristique et IP Reputation

Une fois la configuration de base en place, le tuning avancé permet d'affiner la détection et de réduire les faux positifs/négatifs. Les trois leviers principaux sont le moteur bayésien, les règles heuristiques et la gestion fine de l'IP Reputation.

Moteur bayésien : le filtre bayésien de FortiMail apprend à distinguer le spam du courrier légitime en analysant les tokens (mots, n-grammes) caractéristiques de chaque catégorie. La période de formation initiale dure généralement 2 à 4 semaines pour des environnements avec un volume suffisant (>500 messages/jour). Pour accélérer la formation : exportez un corpus de messages spam connus (format mbox) et importez-les dans la base bayésienne via *Anti-Spam > Bayesian > Import Spam Messages*. Faites de même pour les messages légitimes.

Vérification de l'état du moteur bayésien en CLI :

```
diagnose antispam bayesian status
diagnose antispam bayesian stats
```

Le ratio spam/ham dans la base d'entraînement doit être équilibré (1:1 à 3:1 maximum) pour éviter un biais. Un moteur entraîné sur trop de spam classifiera abusivement les emails légitimes.

Analyse heuristique : FortiMail embarque un ensemble de règles heuristiques (patterns de contenu, en-têtes suspects, structure HTML anormale) qui contribuent au score global. Vous pouvez consulter et ajuster les règles dans *Anti-Spam > Heuristic > Rules*. Évitez de désactiver des règles sans avoir analysé leur contribution aux faux positifs — un log de débogage (`diagnose antispam test verbose enable`) montre quelles règles se déclenchent sur chaque message.

IP Reputation locale : en complément de FortiGuard, FortiMail maintient une base d'IP Reputation locale alimentée par vos propres observations. Une IP qui déclenche fréquemment des alertes antispam peut être automatiquement déclassée. Configurez le seuil d'apprentissage dans *Anti-Spam > IP Reputation > Settings*.

Pour les organisations avec des flux email complexes (partenaires EDI, notifications automatiques de plateformes SaaS), il peut être utile d'activer le **Transparent Header Insertion** : FortiMail ajoute des en-têtes X-FortiMail-* dans chaque email traité, permettant d'auditer le moteur de détection qui a déclenché chaque classification. Ces en-têtes sont invisibles pour le destinataire final mais consultables dans les clients email en mode source.

Configuration SMTP avancée : TLS, authentification et relais

La configuration SMTP de FortiMail détermine les conditions dans lesquelles il accepte et relaie les messages. Une configuration SMTP permissive est une faille de sécurité majeure — un relais SMTP ouvert peut être utilisé pour envoyer du spam depuis votre infrastructure, entraînant le blacklisting de vos IPs et une dégradation de la délivrabilité de vos propres emails.

TLS obligatoire sur les connexions entrantes : dans *System > Mail Settings > SMTP > Security*, activez *Require TLS* pour les connexions SMTP entrantes depuis Internet. FortiMail refusera les connexions non chiffrées. Pour les expéditeurs internes qui ne supportent pas TLS (imprimantes, applications legacy), créez une règle d'exception basée sur l'IP source.

Authentification SMTP sortante : les emails sortants doivent être relayés via FortiMail avec authentification pour éviter l'utilisation comme relais ouvert. Configurez la politique de relais dans *Policy > Relay > Relay Pattern* : seules les IPs internes autorisées ou les utilisateurs authentifiés doivent pouvoir relayer via FortiMail.

SMTP Session Limits : configurez des limites sur les connexions par IP pour limiter l'impact des sources de spam légitimes (expéditeurs mal configurés) et des attaques DDoS au niveau SMTP :

```
config system smtp
  set max-connection-per-ip 50
  set max-msg-per-session 100
  set max-recipient-per-msg 50
  set max-rcpt-per-session 200
end
```

Monitoring, logs SMTP et alertes administrateurs

La supervision de FortiMail est indispensable pour détecter les anomalies (pic de spam, tentatives de relais non autorisé, dégradation de la délivrabilité) et maintenir la qualité de la protection dans la durée. FortiMail propose plusieurs niveaux de logs et d'alertes.

Logs disponibles : *Event Log* (actions système, changements de configuration, connexions admin), *History Log* (journal de tous les messages traités avec leur classification finale et les moteurs déclenchés), *Mail Log* (détail SMTP de chaque transaction). Le History Log est le plus utile pour l'analyse antispam : il permet de retrouver un message spécifique et de comprendre pourquoi il a été classifié d'une certaine façon.

Requête de log via CLI pour analyser les rejets du dernier jour :

```
 execute log filter reset
execute log filter field action reject
execute log filter view-lines 100
execute log display
```

Dashboard antispam : *Monitor > Anti-Spam > Statistics* présente les métriques clés : volume total, pourcentage de spam détecté, taux de rejet par moteur, messages en quarantaine, faux positifs signalés. Consultez ce dashboard quotidiennement pendant les deux premières semaines suivant le déploiement pour valider les seuils de classification.

Alertes par email : configurez des alertes automatiques pour les événements critiques dans *System > Notification > Alert Email* : quota quarantaine dépassé, licence FortiGuard expirée, pic de spam anormal (>200 % de la moyenne). Ces alertes doivent être envoyées à une adresse email externe (pas sur le domaine géré par FortiMail lui-même) pour éviter les boucles.

Pour aller plus loin dans la réponse aux incidents de spam, consultez notre guide FortiMail MO-18 : répondre à une vague de spam active.

Cas réel : configuration type pour une ETI française (200 collaborateurs)

Voici une configuration FortiMail de référence pour une ETI française de 200 collaborateurs, avec un serveur Exchange On-Premises, déployée en mode Gateway avec les enregistrements MX pointant vers FortiMail :

Profil antispam "entrant-standard" :

Moteurs actifs : FortiGuard Email Checksum, FortiGuard URI Check, IP Reputation FortiGuard, SPF (action: Quarantine), DKIM (action: Score), DMARC (action: Honor), Heuristique (activé), Bayésien (activé)

Spam Threshold : 100 (défaut), réévaluer après 30 jours de logs

Probable Spam Threshold : 60

Action Spam : Quarantaine système (administrateur)

Action Probable Spam : Quarantaine utilisateur (self-service)

Durée de rétention quarantaine : 14 jours

Rapports quarantaine utilisateur : quotidiens à 08h30

Politique de relais sortant :

Autorisation de relais : plage IP LAN + authentification SMTP (pour les utilisateurs en mobilité)

TLS sortant vers Exchange : requis (STARTTLS)

Signature DKIM sortante : activée pour le domaine primaire

Rapport DMARC envoyé à : `dmarc-reports@[domaine]`

DNSBL configurées : `zen.spamhaus.org` (principale), `bl.spamcop.net` (secondaire).

Cette configuration permet généralement d'atteindre un taux de détection du spam >98 % avec un taux de faux positifs <0.1 % après la période de tuning bayésien. Pour le détail complet de cette mise en oeuvre, voir notre guide de durcissement antispam FortiMail complet et notre référence détection du spam et phishing en français.

FAQ — Configuration Antispam FortiMail

Quelle est la différence entre FortiMail mode Gateway et le connecteur antispam Microsoft 365 ?

Le connecteur antispam Microsoft 365 (Exchange Online Protection) est intégré à la suite Microsoft et protège les boîtes aux lettres hébergées dans le cloud. FortiMail en mode Gateway

se positionne devant Microsoft 365 en modifiant les enregistrements MX pour que les emails passent d'abord par FortiMail avant d'être relayés vers Exchange Online. L'avantage de ce déploiement hybride est une défense en profondeur : FortiMail bloque les menaces avant qu'elles n'atteignent Exchange Online Protection, et son moteur bayésien peut être entraîné sur les spécificités de votre environnement (terminologie métier, partenaires habituels). L'inconvénient est la complexité accrue et le coût supplémentaire de la licence FortiMail. Pour les organisations qui utilisent uniquement Microsoft 365 sans contrainte de conformité spécifique, EOP suffit généralement. Pour les ETI avec des exigences de traçabilité RGPD ou des flux email sensibles, FortiMail apporte une couche de contrôle supplémentaire et une indépendance vis-à-vis de Microsoft.

Comment diagnostiquer pourquoi un email légitime a été mis en quarantaine FortiMail ?

La première étape est de retrouver le message dans le History Log : *Monitor* > *Log* > *History*, filtre sur l'adresse de l'expéditeur ou du destinataire. L'entrée du log indique la raison de la classification (colonne "Reason") et les moteurs déclenchés. Ensuite, activez le débogage verbose pour reproduire l'analyse : `diagnose antispam test verbose enable`, puis forcez le retraitement du message suspect. Les moteurs déclenchés et leurs scores individuels apparaissent en sortie. Les causes les plus fréquentes de faux positifs : IP de l'expéditeur répertoriée dans un DNSBL (souvent un serveur d'hébergement partagé légitime), SPF fail (expéditeur utilisant un sous-domaine non couvert par le SPF), score bayésien élevé (email contenant des termes marketing inhabituels). Après identification de la cause, ajoutez l'expéditeur à la liste blanche ou corrigez la règle incriminée. Consultez notre guide des modes opératoires GUI pour la procédure complète de libération et analyse des faux positifs.

Peut-on utiliser FortiMail avec Ollama ou des LLM locaux pour améliorer la détection de phishing ?

FortiMail 7.4+ propose une intégration expérimentale avec des services d'analyse IA via l'API REST FortiSandbox, mais ne supporte pas nativement les LLM locaux (Ollama, LM Studio). Des architectures hybrides sont possibles : un serveur intermédiaire peut intercepter les emails via milter (protocole de filtrage de contenu compatible Postfix/Sendmail), analyser le corps du message avec un LLM local, et retourner un score à FortiMail via l'API antispam externe. Cette

approche est prometteuse pour la détection de spear phishing sophistiqué (les LLMs détectent mieux les tentatives d'ingénierie sociale que les moteurs basés sur des signatures), mais elle ajoute de la latence (500ms à 2s par message) et nécessite une infrastructure GPU dédiée. Pour les organisations sans GPU, l'analyse via API OpenAI ou Anthropic est une alternative, mais elle implique d'envoyer des métadonnées d'email vers des serveurs externes — vérifiez la conformité RGPD avant déploiement. Cette approche reste à l'état de preuve de concept en 2026 pour la majorité des organisations.

Aller plus loin : guide de durcissement complet FortiMail

Ce guide couvre la configuration antispam de base et avancée. Pour le durcissement complet de FortiMail — sécurisation de l'interface admin, hardening TLS, gestion des certificats, audit de configuration et recommandations ANSSI — consultez notre guide de référence.

Guide de durcissement FortiMail complet →