

MailInBlack-VIRTUAL

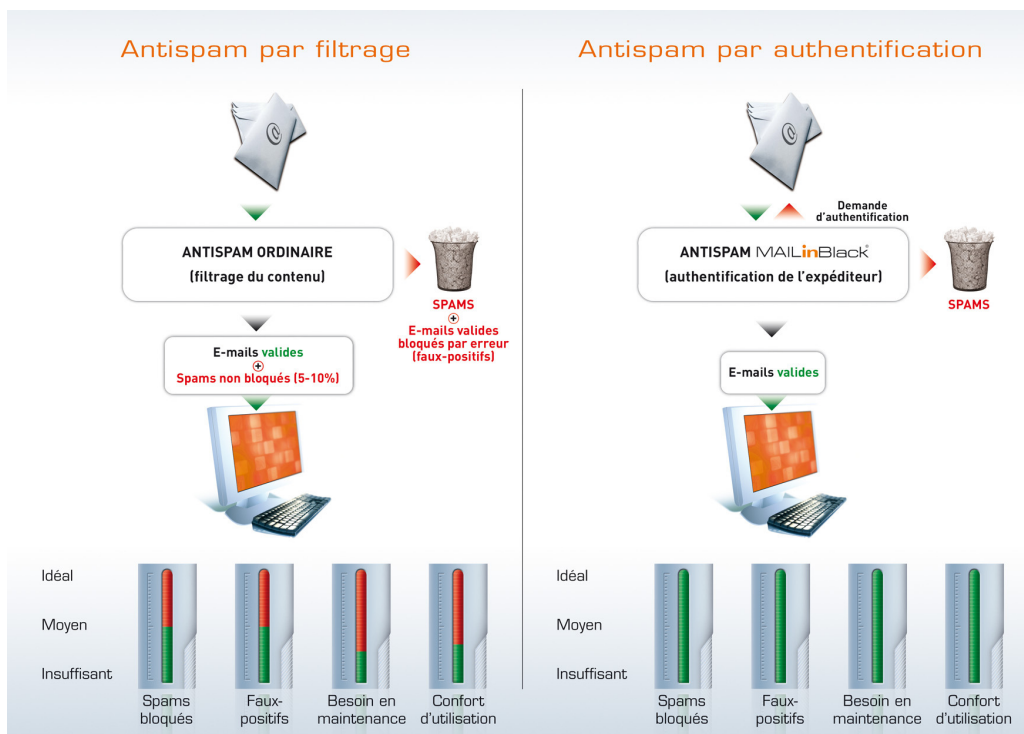
Principe intelligent

- L'antispam MailInBlack contrôle l'identité des expéditeurs et transmet instantanément aux destinataires tous les emails en provenance de contacts connus
- Si occasionnellement un expéditeur n'est pas reconnu, MailInBlack renvoie un message personnel lui demandant de s'authentifier. Simple et rapide, cette opération ne se fait qu'une seule fois. L'expéditeur prouve ainsi qu'il est légitime. Le message est délivré et l'adresse de l'expéditeur est définitivement autorisée
- Les spammers ne répondent pas à la demande d'authentification et tous les spams sont bloqués. Ce principe est imparable et s'adapte à toutes les situations : newsletters, réponses automatiques, double utilisateur protégé...

Bénéfices uniques

Première technologie apportant une confiance totale :

- garantie de recevoir tous ses emails : aucun email valide bloqué par erreur (faux-positif)
- gage de protection absolue : 100% des spams sont stoppés
- élimination de tout travail de monitoring et d'administration lié au spam
- pérennité de la technologie face aux futures techniques de spamming
- antivirus de mail inclus (BitDefender : 120 millions d'utilisateurs dans plus de 100 pays)
- meilleure solution antispam du marché : études comparatives publiées dans L'Express (n°2866) et Micro Hebdo (n°424)



Le produit MailInBlack-VIRTUAL

MailInBlack-VIRTUAL est une solution professionnelle pour les entreprises souhaitant héberger leur applicatif antispam sur un serveur virtuel. Le serveur virtuel doit être installé dans la Dmz du client. Avec MailInBlack-VIRTUAL, l'administrateur gère toute la configuration de sa solution antispam.

Pré-requis matériel

Le serveur virtuel fourni par le client embarque la technologie antispam MailInBlack.

Dans un environnement normal, le serveur virtuel MailInBlack est fonction du nombre de boîtes aux lettres (Bal) total du domaine à protéger. Les pré-requis ci-contre sont indicatifs et peuvent évoluer.

Bal	Processeur	RAM	Disques durs
1 - 200	DC 2,8	512 Mo	1 x 160 Go
1 - 200	DC 3,4	512 Mo	1 x 160 Go
201 - 500	Xéon DC 1,86	1 Go	1 x 160 Go
501 - 1 000	Xéon DC 1,86	1 Go	2 x 160 Go (raid 1)
1 001 - 2 000	Bi-Xéon DC 1,86	2 Go	2 x 146 Go (raid 1)
> 2 000	Bi-Xéon DC 2,00	4 Go	2 x 300 Go (raid 1)

Fonctionnalités spécifiques MailInBlack-VIRTUAL

- **Optimisation** des équipements du client avec un serveur virtuel installé en Dmz
- **Flexibilité d'allocation disque et Ram** et de **déplacement de l'application** sur un autre serveur
- Possibilité de **Snapshot**
- **Synchronisation avec un annuaire d'entreprise** (Ldap ou AD) pour tenir jour les utilisateurs protégés
- **Personnalisation ultime** de l'outil : interface utilisateur (logo différent par domaine si besoin), digest, demande d'authentification (DA 100% personnalisable en html), logo affiché sur la page d'authentification, logo de la page d'accueil de l'interface utilisateur
- **Haute-disponibilité** possible
- **Protection multi-domaines**
- Aucun minimum requis de **licences**
- Choix de services : **sauvegardes, alertes, politique antivirale** (suppression ou désinfection)
- **Surveillance** : monitoring Snmp, contrôles des flux en temps réel, logs, statistiques de trafic
- **Délai de garde des emails stoppés** : paramétrable jusqu'à 45 jours
- **Interface d'administration** de l'appliance et des comptes protégés (modification, pré-autorisation, personnalisation...)

Fonctionnalités communes

- Gestion des **emails automatiques** (newsletter, non-delivery)
- **Confidentialité** de l'email protégé
- **Récapitulatif interactif des emails stoppés** par utilisateur (Digest) envoyé par email : aucun message perdu
- Détection et **refus** des emails reçus pour **des destinataires inconnus**
- **Espace utilisateur** privatif (accès en temps réel aux mails stoppés, pré-autorisation...)
- **Limitation du nombre de demandes d'authentification** (DA) renvoyées :
 - protection des adresses tierces usurpées
 - maîtrise l'envoi de DA à un même expéditeur
 - limite les effets d'une attaque par email
- **Personnalisation** de la DA : logo de l'entreprise, texte partiel, 2 langues
- 6 alias ou groupes de diffusion par licence
- **Pré-autorisation** possible - par l'administrateur ou chaque utilisateur - de contacts connus (par adresse email, domaine ou liste de diffusion)
- Paramétrages : langue (français ou anglais) ; réception des Digests à heures souhaitées...
- Suppression des effets ping-pong

Architecture

MailInBlack-VIRTUAL est placé dans la Dmz en frontal du flux de messagerie entrant, puis pousse les messages validés vers le ou les serveurs de messagerie (un serveur différent possible pour chaque domaine). En cas de présence de relais smtp, il faut que MailInBlack-VIRTUAL soit en amont de tout autre relais. Il faut lui prévoir une adresse IP publique et enregistrer la reverse DNS de cette IP publique. C'est le serveur virtuel qui envoie les demandes d'authentification et c'est sur lui que les expéditeurs se trouvent lorsqu'ils s'authentifient en http.

