

Stratégies de déploiement de MailSecurity

Quel mode de fonctionnement utiliser pour votre réseau

GFI MailSecurity peut être déployé en tant que passerelle SMTP ou en tant que version VS API pour Exchange 2000/2003. Ce livre blanc décrit chaque mode de fonctionnement et vous aide à choisir lequel déployer et si vous devez les déployer tous les deux.

Introduction

Il est possible de déployer GFI MailSecurity en 2 modes de fonctionnement : soit en mode passerelle SMTP soit en version VS API for Exchange 2000/2003. Il peut être utilisé de 3 façons différentes, en utilisant l'un de ces modes ou en utilisant les deux modes simultanément. Ce livre blanc décrit les modes de fonctionnement en détails et vous aide à choisir la meilleure option de déploiement de GFI MailSecurity selon votre réseau.

Introduction.....	2
Pourquoi utiliser les deux modes, Passerelle SMTP et VS API ?.....	2
A propos du mode passerelle SMTP de GFI MailSecurity.....	3
Mode VS API Exchange 2000/2003 pour GFI MailSecurity.....	3
Le déploiement de GFI MailSecurity	5
GFI MailEssentials & GFI MailSecurity sur la même machine.....	7
A propos de GFI Software.....	9

Pourquoi utiliser les deux modes, Passerelle SMTP et VS API ?

GFI MailSecurity est le seul pack de sécurisation de contenu à être compatible avec le mode passerelle SMTP et avec un mode VS API. Pour une sécurisation optimale, nous vous recommandons de déployer les deux. Les deux modes de fonctionnement ont des possibilités qui leurs sont uniques et qui assurent une meilleure sécurisation de votre réseau et de votre serveur de messagerie.

En mode passerelle SMTP, GFI MailSecurity vérifie chaque email entrant et sortant avant qu'ils ne parviennent au serveur de messagerie. Pour que GFI MailSecurity en soit capable, vous devez l'installer devant votre serveur de messagerie (ou sur le Serveur Exchange si vous possédez Exchange 2000/2003). En mode VS API, GFI MailSecurity est installé sur votre Serveur Exchange 2000/2003 et vérifie les messages entrants, sortants ET internes, grâce à l'interface Microsoft VS API.

Si possible, déployez les deux versions. Pour des raisons de gestion et de performance, il est préférable de procéder aux vérifications plus complexes qui prennent plus de temps au niveau de la passerelle. Si vous appliquez ces règles au courrier interne, vous finirez par avoir à modérer beaucoup de messages. Le mode VS API doit toujours être déployé sur le Serveur Exchange pour empêcher une attaque virale de se répandre (qui aurait pu pénétré votre réseau via une disquette, un CD, le Web ou un carnet d'adresses) ou pour surveiller et/ou empêcher les utilisateurs internes de se servir des exploits pour effacer les données. Vous pouvez aussi l'utiliser pour empêcher les utilisateurs non autorisés d'envoyer des pièces jointes exécutables, qu'ils peuvent utiliser pour avoir accès aux informations d'autres utilisateurs qui

eux ont plus de droits sur le réseau.

A propos du mode passerelle SMTP de GFI MailSecurity

Si vous voulez installer GFI MailSecurity sur le périmètre de votre réseau, ou si vous ne possédez pas Microsoft Exchange 2000/2003, vous devez installer GFI MailSecurity en mode passerelle.

En mode passerelle SMTP, GFI MailSecurity vérifie chaque email entrant et sortant avant qu'ils ne parviennent au serveur de messagerie. Pour ce faire, GFI MailSecurity doit être le premier à recevoir les emails destinés à votre serveur de messagerie et il doit constituer la dernière étape pour les messages sortants, par ex., les messages en direction de l'Internet. Pour que cela soit possible, GFI MailSecurity doit être installé en tant que passerelle de messagerie. Cette installation est aussi connue sous le nom de 'Smart host' ou serveur de messagerie relais. GFI MailSecurity agira alors en tant que serveur de messagerie relais.

Mode VS API Exchange 2000/2003 pour GFI MailSecurity

Si vous possédez Microsoft Exchange 2000/2003, GFI MailSecurity est compatible avec Exchange 2000/2003 via le nouveau Microsoft Virus Scanning API (VS API).

Qu'est-ce que VS API (Exchange Virus Scanning API) et à quoi sert-il ?

Exchange 2000/2003 offre un nouveau scan anti-virus API qui est implémenté à un niveau très bas dans la mémoire Exchange. Cela permet à une application de balayage anti-virus d'être très efficace et d'offrir la garantie que le message est balayé avant que les clients puissent y avoir accès ou avant qu'ils puissent ouvrir la pièce jointe. Cet accès à bas niveau facilite l'éradication des virus tels que le virus Melissa.

De plus, VS API réduit les problèmes d'adaptabilité qui surviennent lorsqu'un serveur particulier a un grand nombre d'utilisateurs/boîtes aux lettres. Le scan en temps réel VS API donne la possibilité de scanner les messages et les pièces jointes une fois avant leur livraison, plutôt que autant de fois qu'il y a de boîte aux lettres destinataires. Ce scan unique permet aussi de ne pas scanner à nouveau le message s'il est copié. Pour plus d'informations sur VS API, référez-vous à <http://support.microsoft.com/default.aspx?scid=kb;EN-US;q285667>.

Limitations de l'usage du mode VS API Exchange 2000/2003

Bien que VS API soit recommandé pour la vérification de contenu et anti-virus sur Exchange 2000/2003, il y a plusieurs limitations dont, en tant qu'administrateur de système, vous devriez avoir conscience.

1. Le Scan viral API ne balaye que les informations enregistrées. Cela veut dire que si GFI MailSecurity for Exchange 2000/2003 est installé sur un serveur frontal, par exemple, aucun email ne sera scanné car le message n'aura pas été enregistré sur le serveur

frontal. Dans ce cas vous devez utiliser GFI MailSecurity en mode passerelle SMTP.

2. Vous devez faire plus attention lors du paramétrage des règles des pièces jointes car elles peuvent perturber le trafic interne ; des règles de pièces jointes trop rigoureuses entraînent trop de mises en quarantaine d'emails. De plus, il se pourrait que les applications MAPI exécutées sur Exchange utilisent des fichiers .vbs ou .exe.
3. Les emails sortants qui ont été approuvés doivent être à nouveau envoyés par l'utilisateur. Par exemple, si un exécutable est mis en quarantaine et qu'il est ensuite approuvé, l'utilisateur recevra un message indiquant qu'il/elle a 24h pour renvoyer cet exécutable. La raison est simple, le destinataire du message n'est pas toujours connu à 100% en mode VS API.
4. En mode VS API, le message est divisé en parties. L'interface Exchange VS API transmet les emails à GFI MailSecurity « par morceaux », c'est-à-dire le corps, la pièce jointe 1, la pièce jointe 2, etc. Cela signifie que les parties du message sont mises en quarantaine. Donc, toutes les règles sont appliquées aux parties d'un message. Par exemple, il n'est pas possible de supprimer un email entier s'il a un contenu particulier, mais seulement la partie qui comporte ce contenu.
5. En mode VS API, il peut y avoir un ralentissement des performances lors de la livraison du message. Cela est inévitable car tous les messages doivent être vérifiés avant que l'utilisateur y ait accès. En général, le délai est d'environ 1 seconde (ou moins). Le scan d'un message avec une pièce jointe de 15 Mégaoctets, par exemple, prendra plus longtemps. Chaque solution anti-virus basée sur VS API subira ce ralentissement de performance, toujours est-il que moins les vérifications sont faites, moins la performances ralentira.

Comparaison des modes Passerelle SMTP et VS API

	Passerelle SMTP	VS API
Scans de messages internes	Non	Oui
Scans de messages entrants/sortants	Oui	Oui
Besoin de Windows 2000/XP/2003*	Oui(*)	Oui
Besoin de Active Directory	Non	Oui
Besoin de Exchange 2000/2003	Non	Oui
Traitement en partition des messages	Non	Oui
Exécutable sur la même machine que GFI MailEssentials	Oui	Oui
Exécutable avec Exchange 5.5	Oui	Non
Exécutable avec un serveur Notes ou SMTP	Oui	Non

Exécutable en DMZ ou en serveur relais	Oui	Non
Besoin d'intégration de flux**	Non	Oui
100% de détection de message entrant/sortant ***	Oui	Non

*- Uniquement en mode passerelle

** - La version passerelle SMTP contient plus d'informations sur le message, et peut donc mettre en quarantaine les messages sans avoir besoin du système d'intégration de flux.

*** - La version passerelle SMTP contient plus d'informations sur les emails et peut donc déterminer avec plus de précision s'il s'agit d'un email sortant ou entrant.

Le déploiement de GFI MailSecurity

Option de déploiement 1

Si vous possédez un petit réseau Exchange 2000/2003, et que vous ne désirez pas avoir une messagerie relais séparée en DMZ, utilisez uniquement le mode VS API ; ou si vous préférez uniquement le mode passerelle.

Petits réseaux (par ex., Small Business Server)



Jeu de règles

Mettre en quarantaine les pièces jointes douteuses des messages entrants & sortants

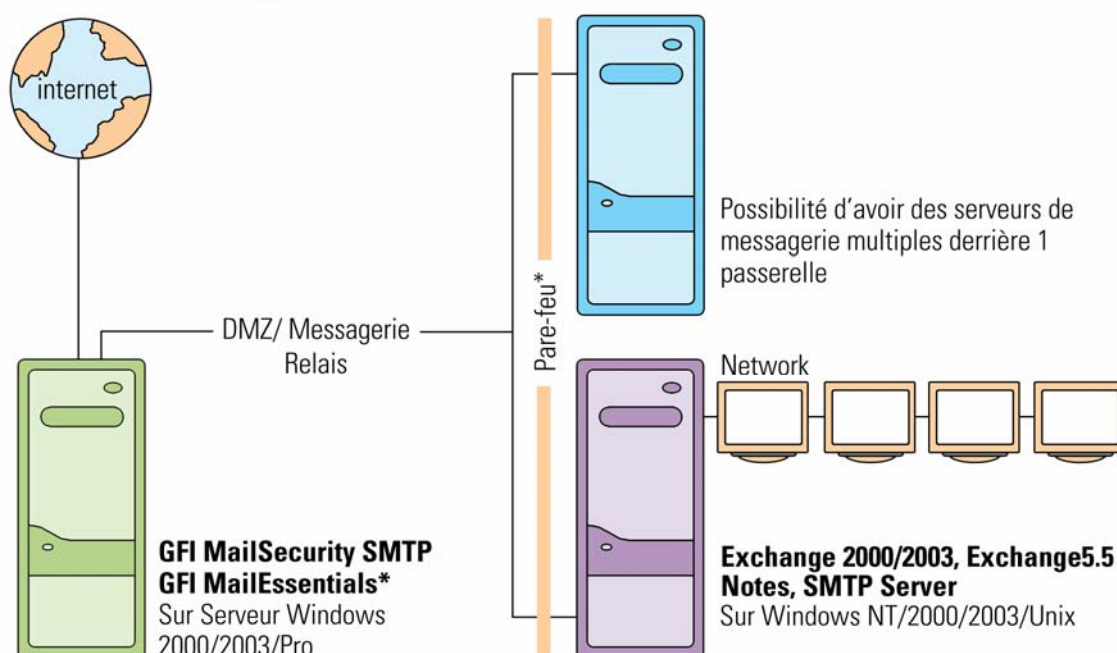
Vérifications virales des messages entrants/ sortants et internes

Moteurs anti-exploit et menaces HTML et Scanner anti-Exécutables et Chevaux de Troie activés *facultatif

Option de déploiement 2

Si vous ne possédez pas Exchange 2000/2003, déployez GFI MailSecurity en mode Passerelle SMTP. Si vous avez Exchange 5.5 Lotus Notes ou un autre serveur SMTP/POP3, vous devez utiliser le mode passerelle SMTP.

Réseaux NT Networks et Windows 2000/2003 pour lesquels GFI MailSecurity n'a pas besoin de sécuriser le réseau interne



Jeu de règles

Mettre en quarantaine les pièces jointes douteuses des messages entrants & sortants *facultatif
Vérifications virales des messages entrants/ sortants et internes
Moteurs anti-exploit et menaces HTML et Scanner anti-Exécutables et Chevaux de Troie activés

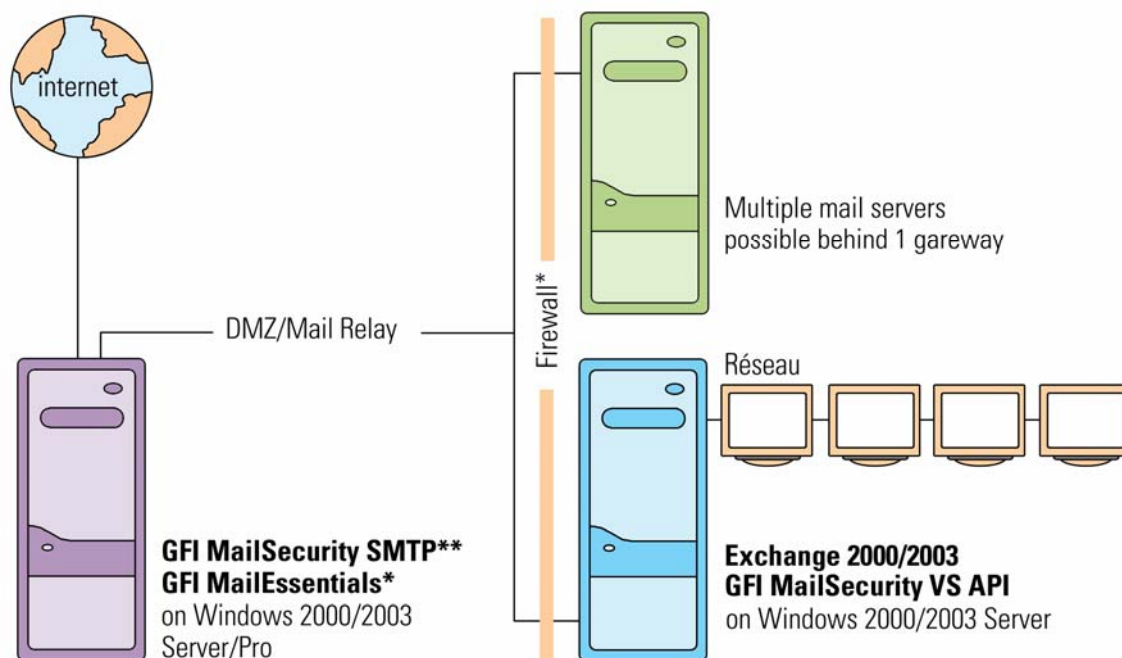
Option de déploiement 3

Si vous possédez un large réseau avec un serveur Exchange 2000/2003 ou plus, nous vous recommandons de déployer GFI MailSecurity sur la machine Exchange 2000/2003 en mode VS API ainsi que sur le périmètre de votre réseau en mode passerelle SMTP. Ci-dessous, le déploiement idéal : l'avantage principal de ce déploiement est que les règles sont plus strictes sur les messages entrants et sortants, et moins strictes sur les messages internes.

Réseaux Windows 2000/2003 plus larges

Situation idéale – Déployez les deux !

1. Utilisez la passerelle sur DMZ pour arrêter toutes les menaces au niveau de la passerelle et contrôler les données qui sortent de votre système
2. Utilisez VS API pour contrôler les apparitions de virus internes



Jeu de règles

Mettre en quarantaine les pièces jointes douteuses des messages entrants & sortants
 Vérifications virales des messages entrants/ sortants et internes
 Moteurs anti-exploit et menaces HTML et Scanner anti-Exécutables et Chevaux de Troie activés

Jeu de règles

Vérification virale interne

*facultatif

**ce paramétrage fait augmenter le prix de la maintenance jusqu'à 30% pour couvrir la licence supplémentaire du moteur antivirus

GFI MailEssentials & GFI MailSecurity sur la même machine

GFI Mail essentials et GFI MailSecurity sont des produits complémentaires qui peuvent être aisément exécutés sur la même machine. GFI MailEssentials apporte des utilitaires de messagerie essentiels à votre Serveur Exchange dont un anti-spam, des disclaimers, une fonction d'archivage de courrier, un système de rapports de messagerie Internet, de réponses automatiques basées sur le serveur et de téléchargement POP3. Un tarif bundle est applicable

lorsque GFI MailSecurity et GFI MailEssentials sont achetés en même temps.

A propos de GFI Software

GFI est l'un des leaders dans le domaine de la réalisation de logiciels qui fournit une seule source intégrée permettant aux administrateurs de résoudre les problèmes de sécurisation de réseaux, de contenu et de messageries. Grâce à sa technologie innovatrice, une stratégie agressive de commercialisation et sa concentration sur le marché de petites et moyennes entreprises, GFI répond aux besoins de continuité d'affaires et de productivité des entreprises et d'autres organisations sur une grande échelle. Fondée en 1992, GFI est une entreprise internationale qui possède des bureaux à Malte, à Londres, Raleigh, Hong Kong, Adelaïde et à Hambourg avec plus de 200.000 installations de ses logiciels à travers le monde. GFI est une entreprise spécialisée et possède un réseau de plus de 10.000 partenaires à travers le monde. Partenaire stratégique de Microsoft, GFI est membre certifié du partenariat Microsoft Gold Certified Partner. Pour plus d'informations à propos de GFI, visitez le site <http://www.gfsfrance.com>.

© 2007 GFI Software. Tous droits réservés. L'information contenue dans ce document représente le point de vue actuel de GFI sur les questions abordées à la date de sa publication. Etant donné que GFI doit répondre aux conditions dynamiques du marché, il ne devrait pas être interprété comme un engagement de la part de GFI, et GFI ne peut pas garantir l'exactitude d'aucune information présentée après la date de la publication. Ce livre blanc est seulement à titre informationnel. GFI NE FAIT AUCUNE GARANTIE, EXPRESSE OU IMPLICITE, DANS CE DOCUMENT. GFI, GFI EndPointSecurity, GFI EventsManager, GFI FAXmaker, GFI MailEssentials, GFI MailSecurity, GFI MailArchiver, GFI LANguard, GFI Network Server Monitor, GFI WebMonitor et leurs logos de produit sont des marques déposées ou des brevets commerciaux de GFI Software aux Etats-Unis et/ou dans d'autres pays. Tous les noms de produit ou d'entreprises mentionnés ci-dessus peuvent être les marques déposées de leurs propriétaires respectifs.