
Estrategias de implementación de GFI MailSecurity

Qué modo(s) operativos usar en su entorno de red

GFI MailSecurity puede ser implementado como gateway SMTP o en versión VS API para Exchange 2000/2003. Este documento describe cada modo operativo y le ayuda a decidir qué implantar y si debe implantar ambos.

Introducción

GFI MailSecurity puede implementarse en 2 modos operativos: Como gateway SMTP o en versión VS API para Exchange 2000/2003. Puede utilizarse de tres formas, bien usando uno de esos modos o utilizando ambos a la vez. Este documento describe en detalle los modos operativos de GFI MailSecurity y le ayuda a elegir la mejor forma de implementar GFI MailSecurity en su red.

Introducción	2
¿Por qué utilizar ambos modos VS API y gateway SMTP?.....	2
Acerca de GFI MailSecurity en modo SMTP gateway	2
GFI MailSecurity en modo Exchange 2000/2003 VS API	3
Cómo implementar GFI MailSecurity	5
GFI MailEssentials y GFI MailSecurity funcionando sobre el mismo equipo.....	7
Acerca de GFI	8

¿Por qué utilizar ambos modos VS API y gateway SMTP?

GFI MailSecurity es el único paquete de seguridad de contenido de correo electrónico que admite ambos modos SMTP gateway y VS API. Para una seguridad óptima, recomendamos implantar ambos. Esto es porque ambos modos operativos tienen capacidades únicas que le permiten asegurar mejor la seguridad de su red y de su servidor de correo.

En el modo gateway SMTP, GFI MailSecurity analiza todo el correo entrante y saliente antes de que alcance su servidor de correo. Para que GFI MailSecurity haga esto, debe instalarlo frente a su servidor de correo (o en el servidor Exchange Server si tiene Exchange 2000/2003). En el modo VS API, GFI MailSecurity se instala en su Exchange 2000/2003 Server y comprueba el correo entrante, saliente e interno, utilizando el interfaz Microsoft VS API.

Si es posible, debe implantar ambas versiones. Por razones de administración y rendimiento, es mejor realizar las comprobaciones más complejas e intensivas en tiempo a nivel de gateway. Si aplicase estas reglas al correo interno, acabaría teniendo que moderar mucho correo. Sin embargo, el modo VS API todavía debe ser implantado en el servidor Exchange, para poder detener la propagación de un brote de virus (que podría haber entrado en su red vía disquete, CD, Web o portátil) o para poder monitorizar y/o detener a usuarios internos que utilizan el correo para extraer datos. Además puede utilizarlo para prevenir que usuarios no autorizados envíen adjuntos ejecutables, que podrían utilizar para obtener información de usuarios que tienen más derechos en la red.

Acerca de GFI MailSecurity en modo SMTP gateway

Si desea instalar GFI MailSecurity en el perímetro de su red, o si no tiene Microsoft Exchange

2000/2003, debe instalar GFI MailSecurity en modo gateway SMTP.

En el modo gateway SMTP, GFI MailSecurity analiza todo el correo entrante y saliente antes de que alcance su servidor de correo. Para hacer esto, GFI MailSecurity debe ser el primero que reciba todos los correos dirigidos a su servidor y deberá ser el último que “detenga” el correo saliente, es decir, los correos dirigidos a Internet. Para que esto ocurra, GFI MailSecurity debe actuar como un gateway para todo el correo. Esta configuración se conoce también como “Host inteligente” o servidor “Retransmisor de correo”. En efecto, GFI MailSecurity actuará como un servidor de retransmisión de correo.

GFI MailSecurity en modo Exchange 2000/2003 VS API

Si dispone de Microsoft Exchange 2000/2003, GFI MailSecurity puede integrarse con Exchange Server 2000/2003 a través de la Microsoft Virus Scanning API (VS API).

¿Qué es y por qué usar VS API (Exchange Virus Scanning API)?

Exchange 2000/2003 proporciona una nueva API de búsqueda de virus que se implementa a muy bajo nivel en el almacén de Exchange. Esto permite a la aplicación de búsqueda de virus ejecutarse con alto rendimiento y garantiza que el mensaje se analizará antes de que cualquier cliente pueda acceder al mensaje o adjunto. Este acceso de bajo nivel facilita la eliminación de virus como el Melissa.

Además, la VS API reduce los problemas de escalabilidad que pueden aparecer cuando un determinado servidor tiene un gran número de usuarios/buzones. El análisis en tiempo real VS-API permite que los mensajes y adjuntos sean analizados antes de ser entregados, en lugar de varias veces determinadas por el número de buzones a los que el mensaje ha de ser entregado. Este análisis en una sola instancia ayuda también a prevenir que los mensajes sean reanalizados cuando se copia un mensaje. Para más información acerca de VS API, lea <http://support.microsoft.com/default.aspx?scid=kb;EN-US;q285667>.

Limitaciones de uso del modo VS API Exchange 2000/2003

A pesar de que la VS API es la forma recomendada de realizar el análisis de contenido y antivirus en Exchange 2000/2003, hay varias limitaciones de las que debe ser consciente como administrador del sistema:

1. La Virus Scanning API analiza sólo los almacenes de información. Esto significa que si ha instalado GFI MailSecurity for Exchange 2000/2003 en, por ejemplo, un servidor front end, no se analizará ningún correo, debido a que éste no está siendo almacenado en el servidor front end. En este caso, necesita utilizar GFI MailSecurity en modo gateway SMTP.
2. Necesita ser mucho más cuidadoso con la aplicación de reglas de adjuntos ya que éstas podrían afectar el tráfico interno; reglas de adjuntos que sean demasiado rígidas pueden suponer demasiado correo en cuarentena. Además, algunas aplicaciones MAPI que se

ejecutan en Exchange podrían estar utilizando archivos vbs o exe.

3. El correo saliente que ha sido aprobado necesita ser reenviado por el usuario. Por ejemplo, si un ejecutable es puesto en cuarentena y aprobado, el usuario recibirá un mensaje advirtiéndole que tiene 24 horas para enviar ese ejecutable. La razón de esto es que el destinatario del mensaje no siempre se conoce con un 100% de certeza en el modo VS API.
4. En el modo VS API, el correo se procesa por partes. El interfaz Exchange VS API pasa el correo a GFI MailSecurity por parte del mensaje, es decir, cuerpo, adjunto 1, adjunto 2, etc. Esto significa que se ponen en cuarentena partes del mensaje, no el mensaje completo. Por lo tanto, todas las seglas son aplicadas a una parte del mensaje. Por ejemplo, usted no puede eliminar un correo completo si tiene un contenido concreto, sino sólo la parte del mensaje que tiene ese contenido.
5. En el modo VS API, ocurrirá algún decremento del rendimiento en la entrega del correo. Esto es inevitable ya que todo correo tiene que ser analizado antes de que lo acceda el usuario. Normalmente, el retardo es aproximadamente 1 segundo o menos, pero un correo con un adjunto de 15 megabytes, por ejemplo, podría tomar más tiempo en ser analizado. Cada solución anti-virus basada en VS API sufrirá este decremento del rendimiento, aunque por supuesto cuantas menos comprobaciones se hagan, menos decremento de rendimiento habrá.

Comparación entre los modos Gateway SMTP y VS API

	SMTP gateway	VS API
Analiza el correo interno	No	Si
Analiza el correo entrante/saliente	Si	Si
Requiere Windows 2000/XP/2003*	Si (*)	Si
Requiere Directorio Activo	No	Si
Requiere Exchange 2000/2003	No	Si
El correo se procesa en partes	No	Si
Funciona en el mismo equipo GFI MailEssentials	Si	Si
Funciona si tiene Exchange 5.5	Si	No
Funciona si tiene Notes o servidor SMTP	Si	No
Funciona en la DMZ o como relanzador de correo	Si	No
Sistema de tickets necesario **	No	Si
Detección de correo entrante/interno al 100%***	Si	No

* - Solo en el gateway

** - La versión Gateway SMTP tiene más información acerca del correo y puede por tanto poner en cuarentena el correo saliente sin necesidad de un sistema de etiquetado.

*** - La versión Gateway SMTP tiene más información acerca del correo y puede por tanto determinar

mejor si es un correo entrante o saliente.

Cómo implementar GFI MailSecurity

Opción de implementación 1

Si tiene una pequeña red Exchange 2000/2003, y no quiere tener un retransmisor de correo aparte en la DMZ, utilice sólo el modo VS API; o si lo prefiere sólo el modo Gateway.

Smaller networks (eg., Small Business Server)



Rule Set

Quarantine inbound & outbound suspicious attachments

Inbound & outbound and internal virus checking

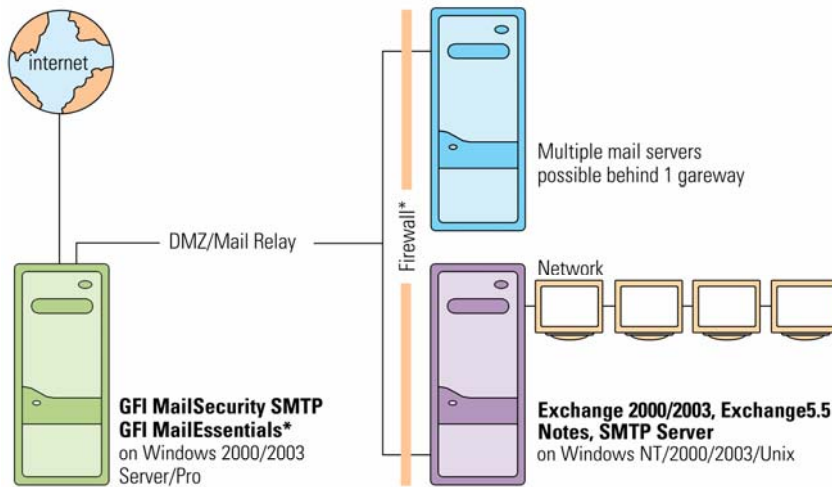
Exploit and HTML threats engines and Trojan & Executable Scanner enabled

*optional

Opción de implementación 2

Si no tiene Exchange 2000/2003, implemente GFI MailSecurity en modo Gateway SMTP. Por lo tanto si tiene Exchange 5.5, Lotus Notes u otro servidor SMTP/POP3, debe utilizar el modo gateway SMTP.

NT Networks and Windows 2000/2003 networks where GFI MailSecurity does not have to secure internal network



Rule Set

Quarantine inbound & outbound suspicious attachments
 Inbound & outbound and internal virus checking
 Exploit and HTML threats engines and Trojan & Executable Scanner enabled

*optional

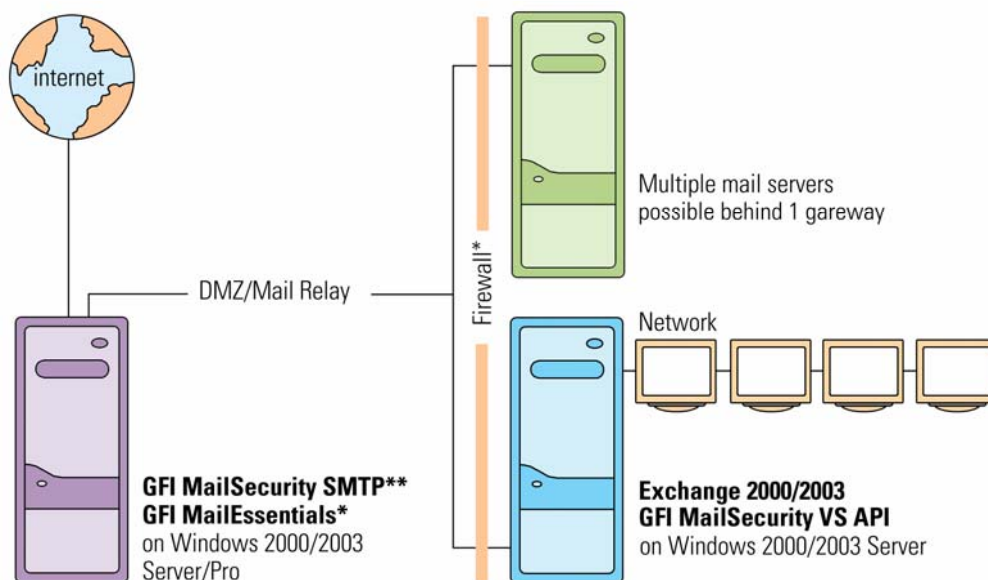
Opción de implementación 3

Si tiene una red más grande con uno o más servidores Exchange 2000/2003, recomendamos implantar GFI MailSecurity tanto en el equipo Exchange 2000/2003 en modo VS API, como en el perímetro de su red en modo Gateway SMTP. Este es el escenario de implementación ideal: la principal ventaja de esta implementación es que se pueden tener reglas estrictas para el correo entrante y saliente, y menos estrictas para el correo interno.

Larger Windows 2000/2003 networks

Ideal Situation - Deploy both!

1. Use gateway on DMZ to stop threats at the gateway and control what data leaves your company
2. Use VS API to control internal virus outbreaks



Rule Set

Quarantine inbound & outbound suspicious attachments
Inbound & outbound and internal virus checking
Exploit and HTML threats engines and
Trojan & Executable Scanner enabled

Rule Set

Internal virus checking

*optional

** this set-up increases maintenance charge to 30% to cover extra virus engine license

GFI MailEssentials y GFI MailSecurity funcionando sobre el mismo equipo

GFI Mail essentials y GFI MailSecurity son productos complementarios y pueden funcionar fácilmente en el mismo equipo. GFI MailEssentials agrega herramientas esenciales a su servidor Exchange incluyendo anti-spam, avisos corporativos, archivo de correo, informes de correo de Internet, auto respuestas basadas en servidor y descarga POP3. Se aplica un precio especial cuando se adquieren juntos GFI MailSecurity y GFI MailEssentials.

Acerca de GFI

GFI es un destacado desarrollador de software que proporciona una única fuente para que los administradores de red dirijan sus necesidades en seguridad de red, seguridad de contenido y mensajería. Con una galardonada tecnología, una agresiva estrategia de precios y un fuerte enfoque en las pequeñas y medianas empresas, GFI es capaz de satisfacer la necesidad de continuidad y productividad de los negocios que tienen las organizaciones en una escala global. Fundada en 1992, GFI tiene oficinas en Malta, Londres, Raleigh, Hong Kong, Adelaide y Hamburgo que soportan más de 200.000 instalaciones en todo el mundo. GFI es una empresa enfocada a canal con más de 10.000 partners en todo el mundo. GFI es también Microsoft Gold Certified Partner. Se puede encontrar más información sobre GFI en <http://www.gfihispana.com>.

© 2007 GFI Software. Todos los derechos reservados. La información contenida en este documento representa la visión del momento de GFI sobre lo discutido a la fecha de la publicación. Como GFI debe responder a las condiciones de los cambios del mercado, no debe ser interpretado como obligación por parte de GFI, y GFI no puede garantizar la exactitud de la información presentada después de la fecha de publicación. Este Documento Blanco solo tiene propósito informativo. GFI NO DA GARANTIA, EXPRESA O IMPLICITAMENTE, EN ESTE DOCUMENTO. GFI, GFI EndPointSecurity, GFI EventsManager, GFI FAXmaker, GFI MailEssentials, GFI MailSecurity, GFI MailArchiver, GFI LANguard, GFI Network Server Monitor, GFI WebMonitor y sus logotipos son marcas registradas o marcas de GFI Software en los Estados Unidos y/o otros países. Todos los nombres de producto o empresas mencionados pueden ser marcas registradas de sus respectivos propietarios.

