

---

## **Strategie d'impiego di GFI MailSecurity**

---

Quale/i modalità operativa/e utilizzare nel proprio ambiente di rete

GFI MailSecurity può essere impiegato come gateway SMTP o come versione VS API per Exchange 2000/2003. Questa white paper descrive le due modalità operative e aiuta a decidere quale impiegare o se utilizzarle entrambe.

---

## Introduzione

GFI MailSecurity può essere impiegato in due modalità operative: come gateway SMTP oppure come versione VS API per Exchange 2000/2003. Si può utilizzare in 3 modi: con ciascuna modalità singolarmente presa oppure usandole entrambe contemporaneamente. Questo documento descrive in dettaglio le modalità operative di GFI MailSecurity ed aiuta a scegliere il modo d'impiego del prodotto più adeguato alla propria rete.

Introduzione.....	2
Perché utilizzare sia la modalità VS API sia quella gateway SMTP? .....	2
Informazioni sulla modalità gateway SMTP di GFI MailSecurity.....	3
Modalità VS API Exchange 2000/2003 di GFI MailSecurity .....	3
Come impiegare GFI MailSecurity .....	5
GFI MailEssentials e GFI MailSecurity in esecuzione sulla stessa macchina .....	7
Informazioni su GFI.....	8

---

## Perché utilizzare sia la modalità VS API sia quella gateway SMTP?

GFI MailSecurity è l'unico pacchetto per la sicurezza del contenuto della posta elettronica a supportare sia la modalità gateway SMTP sia quella VS API. Ai fini di una sicurezza ottimale, raccomandiamo l'impiego di entrambe. Questo perché le due modalità operative sono munite di capacità esclusive che consentono di garantire una migliore sicurezza e della rete e del server di posta.

In modalità gateway SMTP, GFI MailSecurity controlla tutta la posta in entrata e in uscita prima che raggiunga il proprio server di posta. Perché GFI MailSecurity faccia questo, bisogna installarlo davanti al server di posta (o sul server Exchange se si dispone di Exchange 2000/2003). Nella modalità VS API, GFI MailSecurity viene installato sul server Exchange 2000/2003 e controlla la posta in entrata, uscita E quella interna, utilizzando l'interfaccia Microsoft VS API.

Ove possibile, si dovrebbero impiegare entrambe le versioni. Per motivi di amministrazione e prestazioni, è meglio eseguire controlli più complessi ed intensivi a livello di gateway. Se si applicassero tali regole alla posta interna, si finirebbe per dover approvare molte email. Tuttavia, la modalità VS API andrebbe ancora impiegata su Exchange Server, così da fermare la diffusione di virus (che potrebbero essere entrati nella rete mediante floppy, CD, Web o computer portatili) ovvero per monitorare e/o impedire agli utenti interni di utilizzare gli exploit di posta elettronica per sottrarre illegalmente informazioni. Si può anche usare per impedire ad utenti non autorizzati di inviare allegati eseguibili, che possono utilizzare per ottenere

informazioni da utenti muniti di maggiori diritti sulla rete.

---

## **Informazioni sulla modalità gateway SMTP di GFI MailSecurity**

Se si desidera installare GFI MailSecurity lungo il perimetro della propria rete ovvero se non si possiede Microsoft Exchange 2000, bisogna installare GFI MailSecurity in modalità gateway SMTP.

In modalità gateway SMTP, GFI MailSecurity controlla tutta la posta in entrata e in uscita prima che raggiunga il proprio server di posta. Per far ciò, GFI MailSecurity deve essere il primo a ricevere tutti i messaggi destinati al proprio server di posta e l'ultima "fermata" per la posta in uscita, ossia, per i messaggi diretti a Internet. Perché ciò avvenga, GFI MailSecurity deve agire da gateway per tutte le email. Questa impostazione è nota anche come 'Smart host' oppure server 'Mail relay' (*'di ritrasmissione della posta'*). GFI MailSecurity funzionerà effettivamente come server di ritrasmissione della posta.

---

## **Modalità VS API Exchange 2000/2003 di GFI MailSecurity**

Se si dispone di Microsoft Exchange 2000 o 2003, GFI MailSecurity può essere integrato con tale Server Exchange tramite Virus Scanning API (VS API) di Microsoft.

### **Cos'è e perché utilizzare VS API (Exchange Virus Scanning API)?**

Exchange 2000 o 2003 offre una nuova API di scansione dei virus che viene implementata ad un livello molto basso dell'archivio d'Exchange. Ciò consente di eseguire un'applicazione di scansione dei virus ad alte prestazioni e garantisce che il messaggio venga sottoposto a scansione prima che un utente possa accedere ad un messaggio o ad un allegato. Questo accesso a basso livello facilita la rimozione di virus quali il virus Melissa.

Inoltre VS API riduce i problemi di scalabilità che possono sorgere quando un determinato server ha un numero di utenti o caselle di posta elevato. La scansione in tempo reale di VS API consente di sottoporre a scansione messaggi e allegati una sola volta prima di consegnarli, anziché più volte, secondo il numero di caselle di posta cui il messaggio è stato spedito. Questa scansione unica contribuisce inoltre ad evitare che i messaggi vengano sottoposti di nuovo a scansione quando l'email viene copiata. Per ulteriori informazioni su VS API, visitare la seguente pagina web: <http://support.microsoft.com/default.aspx?scid=kb;EN-US;q285667>.

### **Limitazioni d'uso della modalità VS API Exchange 2000/2003**

Nonostante VS API sia un metodo raccomandato per eseguire il controllo del contenuto e antivirus su Exchange 2000/2003, esistono alcune limitazioni che bisogna conoscere:

1. La Virus Scanning API sottopone a scansione unicamente archivi di informazioni. Questo significa che se, ad esempio, si è installato GFI MailSecurity for Exchange 2000/2003 su un server front-end, nessun messaggio è sottoposto a scansione perché la posta non viene archiviata sul server front-end. In questo caso, bisogna utilizzare GFI MailSecurity in modalità gateway SMTP.
2. Bisogna prestare più attenzione quando si applicano regole per allegati, in quanto queste possono avere ripercussioni sul traffico interno: se troppo restrittive, possono produrre un numero eccessivo di messaggi di posta messi in quarantena. Inoltre, applicazioni MAPI che funzionano su Exchange potrebbero utilizzare file .vbs o .exe.
3. L'utente dovrà rinviare i messaggi in uscita che sono stati approvati. Per esempio, se un eseguibile è stato messo in quarantena e quindi approvato, l'utente riceverà la comunicazione che ha 24 ore a disposizione per rimandare detto eseguibile. Il motivo è che il destinatario del messaggio non è sempre noto con una certezza del 100% in modalità VS API.
4. In modalità VS API, la posta è elaborata in base a parti del messaggio. L'interfaccia VS API di Exchange trasferisce le email a GFI MailSecurity per parti di messaggio, vale a dire: corpo, allegato 1, allegato 2, ecc. Ciò significa che sono messe in quarantena parti dei messaggi e non i messaggi nella loro interezza. Pertanto, tutte le regole sono valide per una parte del messaggio. Ad esempio, non è possibile cancellare un'intera email, qualora abbia un determinato contenuto, ma solo la parte di messaggio relativa a quel contenuto.
5. In modalità VS API, avviene una riduzione delle prestazioni di consegna dei messaggi. Ciò risulta inevitabile poiché tutta la posta deve essere controllata prima che l'utente possa accedervi. Normalmente, il ritardo è di circa 1 secondo o anche meno, ma un messaggio con un allegato da 15 megabyte, per esempio, può richiedere un tempo di scansione più lungo. Tutte le soluzioni antivirus basate su VS API subiranno tale riduzione delle prestazioni, benché, ovviamente, minore è il numero di controlli effettuati, minore sarà la riduzione.

### Confronto tra la modalità Gateway SMTP e quella VS API

	Gateway SMTP	VS API
Effettua la scansione della posta interna	No	Sì
Effettua la scansione della posta in entrata/uscita	Sì	Sì
Richiede Windows 2000/XP/2003*.	Sì (*)	Sì
Richiede Active Directory	No	Sì
Richiede Exchange 2000/2003	No	Sì
Posta elaborata in base a parti del messaggio	No	Sì
Può funzionare sulla stessa macchina di GFI MailEssentials	Sì	Sì

Può funzionare se si possiede Exchange 5.5	Sì	No
Può funzionare con server Notes o SMTP	Sì	No
Può funzionare in una DMZ oppure come relay di posta	Sì	No
È richiesto un sistema di ticket**	No	Sì
100% di scoperta della posta in entrata/interna	Sì	No

\* - Solo su gateway

\*\* - La versione gateway SMTP contiene maggiori informazioni sull'email e, pertanto, può mettere in quarantena la posta in uscita senza dover ricorrere ad un sistema di ticket.

\*\*\* - La versione gateway SMTP contiene maggiori informazioni sull'email e, pertanto, è in grado di determinare più efficacemente se si tratta di posta in entrata o in uscita.

## Come impiegare GFI MailSecurity

### Opzione d'impiego n. 1

Se si possiede una rete Exchange 2000/2003 piccola e non si vuole un relay di posta separato nella DMZ, utilizzare esclusivamente la modalità VS API o, se si preferisce, esclusivamente la modalità Gateway.

#### Smaller networks (eg., Small Business Server)



#### Rule Set

Quarantine inbound & outbound suspicious attachments

Inbound & outbound and internal virus checking

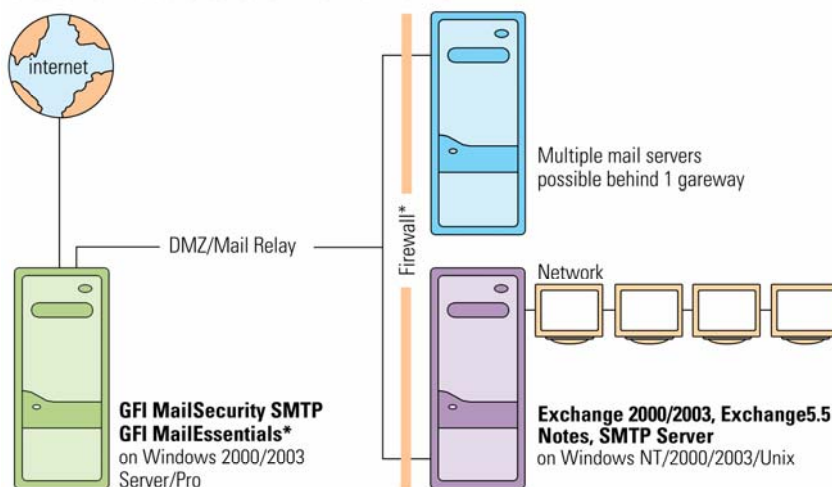
Exploit and HTML threats engines and Trojan & Executable Scanner enabled

\*optional

### Opzione d'impiego n. 2

Se non si dispone di Exchange 2000/2003, impiegare GFI MailSecurity in modalità Gateway SMTP. Si deve altresì utilizzare la modalità gateway SMTP se si dispone di Exchange 5.5, Lotus Notes o un altro server SMTP/POP3.

### 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

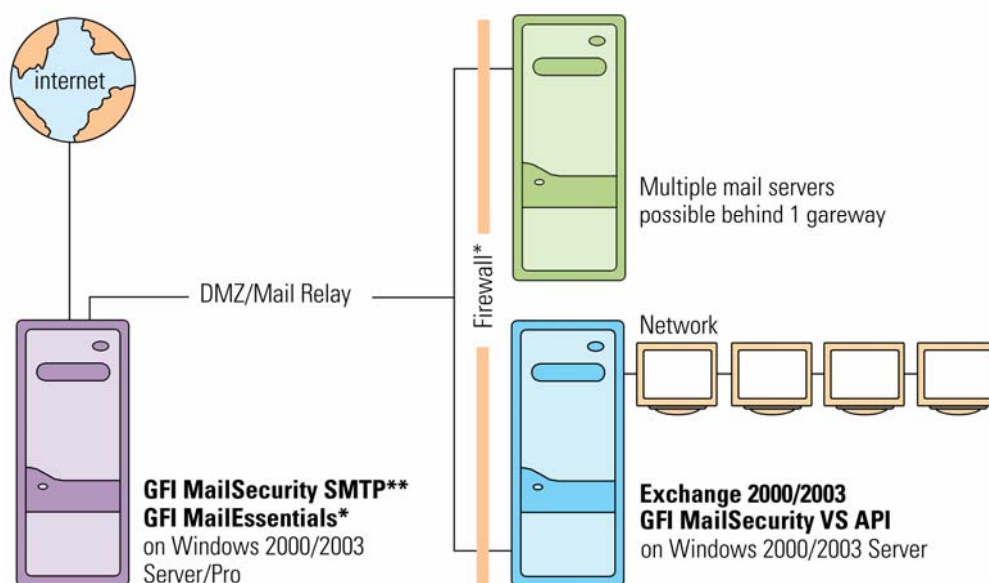
### Opzione d'impiego n. 3

Se si dispone di una rete più estesa con uno o più server Exchange 2000/2003, raccomandiamo l'impiego di GFI MailSecurity in modalità VS API sulla macchina Exchange 2000/2003 e in modalità Gateway SMTP alla periferia della rete. Si tratta dell'impiego ideale di GFI MailSecurity: il vantaggio principale di tale impiego risiede nella possibilità di configurare regole più restrittive per la posta in entrata e in uscita, ovvero regole meno rigide per la posta interna.

## 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 e GFI MailSecurity in esecuzione sulla stessa macchina

GFI Mail essentials e GFI MailSecurity sono prodotti complementari e possono essere eseguiti facilmente sulla stessa macchina. GFI Mail essentials aggiunge fondamentali strumenti per la posta elettronica al server Exchange, compresi anti-spam, disclaimer, archiviazione della posta, rapporti sulla posta Internet, risposte automatiche basate sul server e scaricamento POP3. Vengono applicati speciali prezzi di pacchetto quando si acquistano contemporaneamente GFI MailSecurity e GFI MailEssentials.

---

## Informazioni su GFI

GFI è una società leader nello sviluppo di software, che offre agli amministratori di rete un'unica fonte in grado di soddisfare le loro esigenze di protezione della rete, sicurezza del contenuto e messaggistica. Grazie alla tecnologia vincitrice di numerosi riconoscimenti, ad una politica tariffaria aggressiva e alla particolare attenzione rivolta alle piccole e medie aziende, GFI riesce a soddisfare le esigenze di continuità e produttività aziendali delle organizzazioni in generale. Costituita nel 1992, GFI ha uffici a Malta, Londra, Raleigh, Hong Kong, Adelaide, e Amburgo, a supporto di oltre 200.000 installazioni in tutto il mondo. GFI è orientata alla collaborazione con partner e si avvale infatti di oltre 10.000 partner in tutto il mondo. GFI è inoltre Microsoft Gold Certified Partner. Maggiori informazioni su GFI sono reperibili sul sito <http://www.gfi-italia.com>.

© 2007 GFI Software. Tutti i diritti riservati. Le informazioni contenute nel presente documento rappresentano l'attuale conoscenza della GFI, in merito agli argomenti trattati, alla data di pubblicazione. A causa di cambiamenti nelle condizioni di mercato, non deve essere considerato in alcun modo un impegno da parte di GFI, e GFI non può garantire l'esattezza delle informazioni fornite dopo la data di pubblicazione. Questa white paper deve essere considerata a puri fini informativi. GFI NON OFFRE GARANZIE, ESPLICITE O IMPLICITE, NEL PRESENTE DOCUMENTO. GFI, GFI EndPointSecurity, GFI EventsManager, GFI FAXmaker, GFI MailEssentials, GFI MailSecurity, GFI MailArchiver, GFI LANguard, GFI Network Server Monitor, GFI WebMonitor e i rispettivi loghi sono marchi registrati o marchi di GFI Software negli Stati Uniti e/o in altri paesi. Tutti i prodotti e le aziende nominate nel presente documento sono marchi registrati dei rispettivi proprietari.

