
Inzetmogelijkheden van GFI MailSecurity

Welke versie is het meest geschikt voor uw netwerkomgeving?

GFI MailSecurity is leverbaar als SMTP-gatewayversie en als VS API-versie voor Exchange 2000/2003. Dit white paper beschrijft beide versies en helpt u beslissen welke versie voor u het meest geschikt is en of u beide versies zou moeten gebruiken.

Inleiding

GFI MailSecurity is leverbaar in twee versies: een SMTP-gatewayversie en een VS API-versie voor Exchange 2000/2003. Het kan op drie manieren worden gebruikt, namelijk in een van deze twee versies of door beide versies tegelijk te gebruiken. Dit paper beschrijft de verschillende versies in detail en helpt u beslissen hoe u het best GFI MailSecurity op uw netwerk kunt gebruiken.

Inleiding	2
Waarom zou ik zowel de VS API-versie als de SMTP-gatewayversie gebruiken?.....	2
Over de GFI MailSecurity SMTP-gatewaymodus	2
GFI MailSecurity VS API Exchange 2000/2003-modus	3
Installatie van GFI MailSecurity	5
GFI MailEssentials & GFI MailSecurity op dezelfde machine	7
Over GFI	8

Waarom zou ik zowel de VS API-versie als de SMTP-gatewayversie gebruiken?

GFI MailSecurity is het enige inhoudsbeveiligingspakket voor e-mail dat zowel voor SMTP-gateway als voor VS API leverbaar is. We raden u aan beide versies te gebruiken voor optimale bescherming. Beide versies beschikken namelijk over unieke kwaliteiten waardoor u verzekerd kunt zijn van een betere beveiliging voor uw netwerk en mailservers:

De SMTP-gatewayversie van GFI MailSecurity controleert alle inkomende en uitgaande mail voordat deze uw mailservers bereikt. Om dit mogelijk te maken moet u GFI MailSecurity voor uw mailservers installeren (of, als u Exchange 2000/2003 heeft, op de Exchange Server). De VS API-versie wordt geïnstalleerd op uw Exchange 2000/2003 Server en controleert inkomende, uitgaande EN interne mail in de Microsoft VS API interface.

Indien mogelijk is het het beste om beide versies te gebruiken. Als het om beheer en performance gaat, is het beter om de complexere en meer tijdrovende checks op gatewayniveau uit te voeren. Als u deze regels op interne mail zou toepassen, zou u erg veel mail moeten screenen. De VS API-modus kan echter nog steeds op de Exchange Server worden gebruikt ter voorkoming van de verspreiding van een virus (dat het netwerk binnen kan zijn gekomen via een diskette, een cd, het web of een notebook) of om te voorkomen dat interne gebruikers e-mail exploits gebruiken om aan bepaalde gegevens te komen. U kunt er ook mee voorkomen dat gebruikers uitvoerbare attachments verzenden om informatie te bemachtigen van gebruikers die meer rechten hebben op het netwerk.

Over de GFI MailSecurity SMTP-gatewaymodus

Als u GFI MailSecurity aan de netwerkperimeter installeert, of als u niet over Microsoft

Exchange 2000/2003 beschikt, moet u GFI MailSecurity in SMTP-gatewaymodus installeren.

De SMTP-gatewayversie van GFI MailSecurity controleert alle inkomende en uitgaande mail voordat deze uw mailserver bereikt. Hiervoor moeten alle e-mails die voor uw mailserver bestemd zijn eerst door GFI MailSecurity worden ontvangen. Ook moet GFI MailSecurity de laatste "halte" zijn voor uitgaande mail, dus mailtjes die bestemd zijn voor het internet. Om dit mogelijk te maken moet GFI MailSecurity als gateway voor alle e-mail functioneren. Deze opzet staat bekend als smart host of mail relayserver. GFI MailSecurity werkt in feite als een mail relay server.

GFI MailSecurity VS API Exchange 2000/2003-modus

Als u over Microsoft Exchange 2000/2003 beschikt, kan GFI MailSecurity integreren met Exchange 2000/2003 via de nieuwe Microsoft Virus Scanning API (VS API).

Wat is VS API (Exchange Virus Scanning API) en waarom zou ik het gebruiken?

Exchange 2000/2003 biedt een nieuwe VS API die op een zeer laag niveau in de Exchange store wordt geïmplementeerd. Op deze manier werkt de virusscanner op volledige capaciteit en bent u er zeker van dat elk bericht wordt gescand voordat een client een bericht of attachment kan openen. Deze eenvoudige toegang vergemakkelijkt de eliminatie van virussen zoals het Melissa-virus.

Bovendien reduceert VS API schaalbaarheidsproblemen die kunnen ontstaan wanneer een bepaalde server een groot aantal gebruikers/mailboxen heeft. Met de realtime scan van VS API kunnen berichten en bijlagen voordat ze worden bezorgd één keer worden gescand, in plaats van verschillende malen afhankelijk van het aantal mailboxen waarnaar het bericht wordt gestuurd. Dit eenmalige scannen voorkomt tevens dat berichten opnieuw worden gescand wanneer ze worden gekopieerd. Voor meer informatie over VS API kunt u kijken op <http://support.microsoft.com/default.aspx?scid=kb;EN-US;q285667>

Beperkingen van de VS API Exchange 2000/2003-modus

Hoewel VS API wordt aanbevolen voor het controleren van inhoud en het bestrijden van virussen op Exchange 2000/2003, zijn er enkele beperkingen waarmee u als systeembeheerder rekening moet houden:

1. De VS API scant alleen information stores. Dit betekent dat als GFI MailSecurity for Exchange 2000/2003 op een front-end-server geïnstalleerd staat, er geen mail wordt gescand. De mail is immers niet opgeslagen op de front-end-server. In dit geval moet u GFI MailSecurity in SMTP-gatewaymodus gebruiken.
2. We raden aan voorzichtig te zijn met het toepassen van regels voor attachments: te strenge regels kunnen ertoe leiden dat te veel berichten in quarantaine worden geplaatst.

Bovendien kunnen MAPI-applicaties op Exchange .vbs- of .exe-bestanden gebruiken.

3. Uitgaande berichten die zijn goedgekeurd moeten opnieuw door de gebruiker worden verzonden. Als een uitvoerbaar bestand bijvoorbeeld in quarantaine geplaatst is en goedgekeurd is, ontvangt de gebruiker een bericht waarin staat dat hij of zij 24 uur de tijd heeft om dit uitvoerbare bestand opnieuw te verzenden. De reden hiervoor is dat het in VS API-modus niet altijd 100% zeker is wie de ontvanger van het bericht is.
4. In VS API-modus wordt mail in afzonderlijke onderdelen verwerkt. De Exchange VS API interface geeft berichten per onderdeel door aan GFI MailSecurity, dus de body, attachment 1, attachment 2, enzovoort. Dit betekent dat alleen onderdelen van berichten in quarantaine worden geplaatst, en dus geen volledige berichten. Alle regels worden dus toegepast op elk onderdeel. Een bericht dat gevaarlijke inhoud bevat wordt bijvoorbeeld niet geheel verwijderd, maar alleen het gedeelte met gevaarlijke inhoud.
5. In VS API-modus treedt er enige vertraging op in de bezorging van e-mail. Dit is niet te vermijden aangezien alle berichten moeten worden gecontroleerd voordat ze door de gebruikers worden geopend. Meestal is de vertraging maximaal 1 seconde, maar een voor een bericht met een groot attachment van bijvoorbeeld 15 megabyte zal het scannen meer tijd in beslag nemen. Iedere antivirusoplossing die is gebaseerd op VS API leidt tot enige vertraging. Uiteraard is het zo dat hoe minder controles er worden uitgevoerd, des te minder vertraging er optreedt.

Vergelijking tussen SMTP-Gatewaymodus en VS API-modus

	SMTP-gateway	VS API
Scant interne mail	Nee	Ja
Scant inkomende/uitgaande mail	Ja	Ja
Windows 2000/XP/2003* vereist	Ja (*)	Ja
Active Directory vereist	Nee	Ja
Exchange 2000/2003 vereist	Nee	Ja
Mail wordt per onderdeel gescand	Nee	Ja
Kan op dezelfde machine worden gerund als GFI MailEssentials	Ja	Ja
Werkt met Exchange 5.5	Ja	Nee
Ondersteunt Notes of SMTP-server	Ja	Nee
Kan in DMZ of als mail relay runnen	Ja	Nee
Ticketingsysteem nodig **	Nee	Ja
100% betrouwbare identificatie van inkomende en interne mail***	Ja	Nee

* - Alleen op gateway

** - De SMTP-gatewayversie heeft meer informatie over het bericht en kan dus uitgaande mail in

quarantaine plaatsen zonder dat er een ticketingsysteem nodig is.

*** - De SMTP-gatewayversie heeft meer informatie over het bericht en kan daardoor beter beoordelen of het om een inkomend of een uitgaand bericht gaat.

Installatie van GFI MailSecurity

Installatie-optie 1

Als u een kleiner Exchange 2000/2003 netwerk heeft en geen aparte mail relay in de DMZ wilt, gebruik dan alleen de VS API-modus (of alleen de Gatewaymodus).

Smaller networks (eg., Small Business Server)



Rule Set

Quarantine inbound & outbound suspicious attachments

Inbound & outbound and internal virus checking

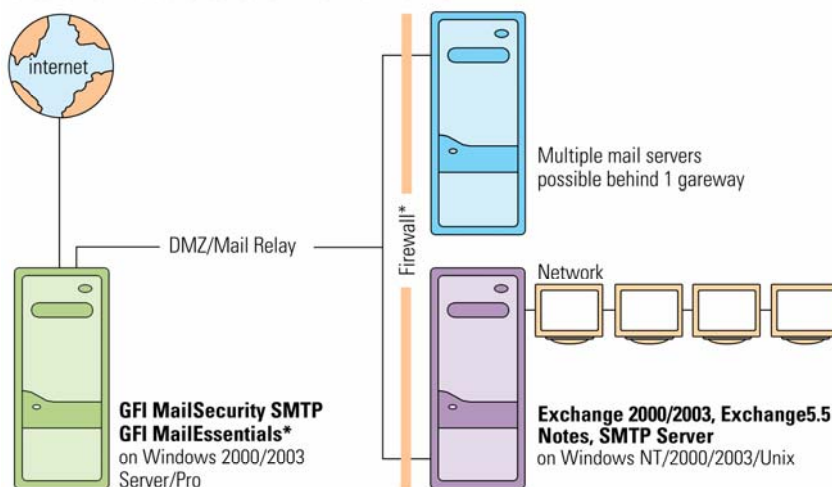
Exploit and HTML threats engines and Trojan & Executable Scanner enabled

*optional

Installatie-optie 2

Als u geen Exchange 2000/2003 heeft, gebruik GFI MailSecurity dan in SMTP-gatewaymodus. Als u dus Exchange 5.5, Lotus Notes of een andere SMTP/POP3 server heeft, moet u de SMTP-gatewaymodus gebruiken.

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

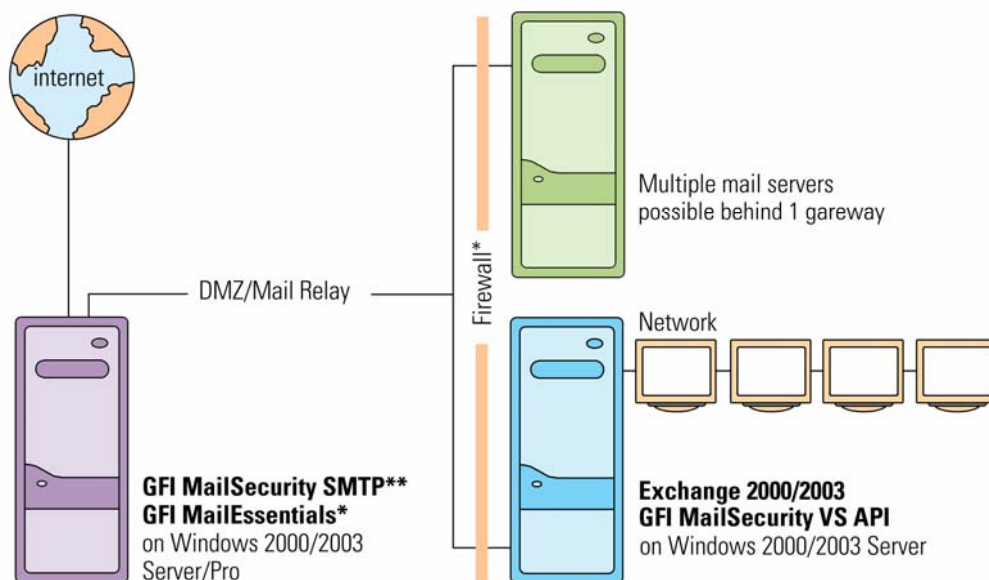
Installatie-optie 3

Als u een groter netwerk heeft met een of meer Exchange 2000/2003 servers, raden we u aan om GFI MailSecurity zowel te installeren op de Exchange 2000/2003 machine in VS API-modus als aan de perimeter van uw netwerk in SMTP-gatewaymodus. Dit is het ideale installatiescenario: het belangrijkste voordeel van deze installatiemethode is dat u strengere regels kunt hebben voor inkomende en uitgaande mail en minder strenge regels voor interne mail.

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 & GFI MailSecurity op dezelfde machine

GFI MailEssentials en GFI MailSecurity zijn zusterproducten en kunnen dus gemakkelijk op dezelfde machine worden geïnstalleerd. GFI MailEssentials voegt belangrijke tools voor e-mail toe aan uw Exchange Server, zoals antispam, disclaimers, e-mailarchivering, Internetmailrapportage, servergebaseerde autoreplies en POP3 downloading. Als u GFI MailSecurity en GFI MailEssentials samen koopt, geldt een speciale bundelprijs.

Over GFI

GFI is een toonaangevende ontwikkelaar van software voor netwerkbeveiliging, inhoudsbeveiliging en messaging. Dankzij bekroonde technologie, een agressieve prijsstrategie en een sterke focus op MKB-bedrijven helpt GFI bedrijven over de hele wereld om maximale continuïteit en productiviteit te bewerkstelligen. GFI is opgericht in 1992 en heeft kantoren in Malta, Londen, Raleigh, Hong Kong, Adelaide en Hamburg die wereldwijd meer dan 200.000 installaties ondersteunen. GFI is een kanaalgericht bedrijf met meer dan 10.000 partners over de hele wereld. GFI is ook een Microsoft Gold Certified Partner. Meer informatie over GFI is te vinden op <http://www.gfi.nl>.

© 2007 GFI Software Ltd. Alle rechten voorbehouden. De informatie in dit document geeft het standpunt van GFI weer betreffende de besproken onderwerpen op de datum van publicatie. Aangezien GFI moet reageren op veranderende marktomstandigheden, moet dit document niet als een toezegging van GFI worden geïnterpreteerd. Na de publicatiedatum kan de correctheid van de informatie niet worden gegarandeerd. Dit white paper dient puur ter informatie. GFI GEEFT IN DIT DOCUMENT GEEN ENKELE GARANTIE, EXPLICIET NOCH IMPLICIET. GFI, GFI EndPointSecurity, GFI EventsManager, GFI FAXmaker, GFI MailEssentials, GFI MailSecurity, GFI MailArchiver, GFI LANguard, GFI Network Server Monitor, GFI WebMonitor en de bijbehorende logo's zijn ofwel geregistreerde handelsmerken of handelsmerken van GFI Software Ltd. in de Verenigde Staten en/of andere landen. Alle product- en bedrijfsnamen in dit persbericht zijn mogelijk handelsmerken van hun respectievelijke eigenaren.