

Avira **AntiVir** MailGate

Support
August 2010



www.avira.de

Irrtümer und technische Änderungen vorbehalten
© Avira GmbH

Inhaltsverzeichnis

<i>1 Installation</i>	3
1.1 Installationspaket näher betrachtet	3
1.2 Tipps zur Installation	4
1.3 Installationsvarianten	5
<i>2 MailGate im Einsatz</i>	7
2.1 MailGate zusammen mit Postfix.....	7
2.2 MailGate zusammen mit Sendmail	9
2.3 MailGate zusammen mit Avira AntiSpam.....	9
2.4 MailGate zusammen mit anderen MTAs.....	9
<i>3 MailGate Suite im Einsatz</i>	10
3.1 Besonderheiten MailGate Suite	10
<i>4 Praxisorientierte Tipps</i>	11
4.1 Log-ging	11
4.2 Konfiguration	11
4.3 Updates.....	14

1 Installation

1.1 Installationspaket näher betrachtet

Sie können das aktuelle MailGate Installationspaket jederzeit von unserer Webseite beziehen:

```
http://www.avira.de/de/downloads/avira_antivir_mailgate.html
```

Bitte entpacken Sie das heruntergeladene Installationspaket wie folgt:

```
$ gzip -cd antivir-mailgate-prof.tgz | tar xvf
```

Das entstandene Verzeichnis beinhaltet ein paar wesentliche Verzeichnisse und Dateien auf die im folgenden näher eingegangen wird.

```
$ cd antivir-mailgate-prof-<Version>
```

```
antivir-mailgate-prof-3.0.0-7-0 #
```

```
.installrc  
LICENSE  
LICENSE.DE  
README  
bin  
contrib  
doc  
etc  
install  
legal  
pgp  
script  
smcpg  
templates  
vdf
```

Das Installationsverzeichnis ist wie folgt gegliedert:

install	- Hauptinstallationskript
.installrc	- Produktinformationsdatei
LICENSE	- Avira GmbH Software License Agreement
doc/RELEASE_NOTES	- wichtige Änderungen dieser Version
README	- Beschreibung Installationspaket
doc/	- Dokumentationen
pgp/	- PGP Schlüssel und Anleitung
bin/	- Ausführbare Dateien
vdf/	- Basisvirendefinitionen
legal/	- Lizenzbestimmungen 3rd-Party Bestandteile
etc/	- Konfigurationsdateien
script/	- Shell Skripte
smcpkg/	- SMC-spezifische Dateien
templates/	- Anwendungsbezogene Templates
contrib/	- 3rd-Party Software

1.2 Tipps zur Installation

Die kommandozeilenorientierte, interaktive Standardinstallation können Sie wie folgt aufrufen:

```
$ ./install
```

Haben Sie bereits eine Installation zu einem früheren Zeitpunkt durchgeführt, können Sie die Installation zusätzlich beschleunigen:

```
$ ./install -fast
```

Unattended Installation

Wenn Sie eine komplett automatische (unattended) Installation durchführen wollen, können Sie die Installationsvariante verwenden, die auch die SMC intern verwendet:

```
$ ./install --fast --inf=./smcpkg/setup.inf
```

Alle Einstellungen für die automatische Installation befinden sich in der angegebenen INF Datei. Sie könnten also auch eine Kopie mit Ihren eigenen Einstellungen verwenden und so zum Beispiel einen größeren Rollout durchführen oder sich einfach die tägliche Arbeit vereinfachen.

./smcpkg/setup.inf:

```
SAVAPI3_ADDLINK=y
MAILGATE_ADDLINK=y
MAILGATE_AUTOSTART=y
MAILGATE_MANPAGESDIR=" "
MAILGATE_LOCALACL="`hostname -f` `hostname -d`"
MAILGATE_RELAYACL="127.0.0.1/8 192.168.0.0/16"
UPDATER_INSTALL=y
UPDATER_ADDLINK=y
UPDATER_ADDCRONJOB=y
UPDATER_CYCLE_SIG_EN=2h
UPDATER_CYCLE_PROD=y
UPDATER_CYCLE=2
UPDATER_EMAILTO=n
SMC_INSTALL=1
ANTIVIR_CONFIG=n
LICENSE_AGREEMENT=y
```

Standardinstallation

Während der Installation werden Ihnen Fragen zur Basiskonfiguration gestellt. Sie können bedenkenlos die Standardwerte verwenden.

1.3 Installationsvarianten

MailGate ist ein dedizierter Mailserverdienst, mit eigenem Queue-Management, der in der Regel über das SMTP-Protokoll mit anderen Mailservern (MTAs) kommunizieren kann. Dadurch gibt es eine Vielzahl an möglichen Kombinationen. In vielen Fällen fungiert MailGate als einfaches Mailrelay mit eingebauter Filterfunktion.

Es gibt derzeit zwei besondere Installationsarten, die eine direkte Integration in einen bestehenden Mailserver zulassen:

- Postfix Content-Filter
- Sendmail Militer

Die Kombination mit Postfix hat sich bei den meisten Kundenfällen bewährt. Sendmail wird in speziellen Fällen und vor allem auf UNIX Systemen wie Solaris eingesetzt.

Welche Variante sollte wann genutzt werden ?

Beide Varianten skalieren sehr gut und werden sowohl auf kleinen Installationen, als auch im Enterprisebereich eingesetzt. Der jeweilige MTA behält dabei die Hauptrolle im Mailverkehr und MailGate wird über eine Umleitung eingebunden, die Bedrohungen wirkungsvoll in die Quarantäne verweisen bzw. direkt abblocken kann (bei Militer).

Der große Vorteil dabei ist, dass alle Optionen, die der MTA sonst bietet (SMTP-AUTH etc.), erhalten bleiben. MailGate selbst, ist aufgrund seiner Funktion, auf Basiskommandos des SMTP-Protokolls beschränkt.

MailGate „Standalone“ als Relay

Die klassische Variante - MailGate als einfaches Mailrelay - kann zum Beispiel im Enterprisebereich sehr interessant sein, da es dort oft deutlich komplexere Mailstrukturen gibt.

Außenstellen, Hochverfügbarkeit und Redundanzen machen es in der Theorie nötig, MailGate mehrfach zu installieren. Somit steigt auch der administrative Mehraufwand. Bewährt hat sich daher in einer solchen Umgebung, MailGate als zentrales Relay, z.B. innerhalb der firmenweiten DMZ, einzusetzen.

Ein Beispiel:

```
Internet → externer MX → Firewall → MailGate (DMZ)
      → Firewall → interner Mailrelay → interne Infrastruktur
```

2 MailGate im Einsatz

2.1 MailGate zusammen mit Postfix

MailGate vor Postfix

Eine relativ selten eingesetzte, aber sehr einfach umzusetzende Variante ist die Möglichkeit, MailGate als lokales Relay, vor Postfix zu verwenden.

Schema für diese Konfiguration:

Internet → MailGate → Postfix → weiterer MTA / Client (MUA)

Eine genaue Installationsbeschreibung, dieser Konfigurationsvariante, finden Sie im MailGate Handbuch, auf Seite 30 (Port 25 überwachen).

MailGate als Content Filter

MailGate kann in Verbindung mit Postfix als sogenannter Content Filter eingebunden werden. Diese Konstellation ist die am häufigsten anzutreffende Lösung bei unseren Kunden. Eine Installation ist relativ einfach. Postfix bringt die Unterstützung für Content Filter in der Regel bereits mit.

Schema für diese Konfiguration:

Internet → Postfix → [UMLEITUNG] → MailGate → [FORWARD] →
→ Postfix Backdoor → weiterer MTA / Client (MUA)

In der Hauptkonfiguration von Postfix (main.cf) wird lediglich der Eintrag für den Content Filter (die Umleitung) erfasst:

"antivir" = Port 10024

/etc/postfix/main.cf:

```
content_filter=smtpl:localhost:10024
```

Im Folgenden wird in der Dienstkonfiguration von Postfix ein weiteres TCP-Socket definiert, auf dem der bekannte Mailserverdienst "smtpd" lauschen soll. Wichtig ist dabei, dass die vormals global gültige Definition für den Content Filter wieder zurückgesetzt wird, damit keine Mailschleife entsteht.

"smtp-backdoor" = Port 10025

/etc/postfix/master.cf:

```
localhost:10025 inet n - n - - smtpd -o content_filter=
```

Postfix sollte danach neu gestartet werden, damit die Konfiguration übernommen wird. Damit ist die Konfiguration in Postfix erledigt.
Die MailGate Konfiguration ist ebenfalls sehr einfach:

/etc/avmailgate.conf:

```
ListenAddress localhost port 10024  
ForwardTo SMTP: localhost port 10025
```

Auch hier ist im Anschluss ein MailGate Neustart erforderlich, um die Konfiguration zu übernehmen.

2.2 MailGate zusammen mit Sendmail

Eine interessante Einsatzvariante ist die Einbindung über die Sendmail Milter Schnittstelle.

Schema für diese Konfiguration:

```

Internet
  |
Sendmail ↔ [MILTER] ↔ MailGate
  |
weiterer MTA / Client (MUA)

```

Tipp: Bei dieser Variante ist es möglich, direkt im SMTP-Dialog eine Mail zu überprüfen und im Falle eines Fundes direkt abzulehnen, also ein direktes „REJECT“ zu ermöglichen.

Eine genaue Installationsanleitung ist im MailGate Handbuch, ab Seite 15 zu finden.

2.3 MailGate zusammen mit Avira AntiSpam

Die Inhouse-Lösung von Avira AntiSpam kann ideal mit MailGate kombiniert werden und bietet einen effektiven Schutz vor der täglichen Spamflut.

Eine Kombination ist möglich als:

- erweiterter Content Filter
- Standalonebetrieb beider Produkte

2.4 MailGate zusammen mit anderen MTAs

MailGate kann grundsätzlich mit jedem Mailserver agieren, der RFC-konform SMTP spricht. Typische Kombinationen sind:

- MailGate + Exim
- MailGate + Qmail
- MailGate + Exchange

Um MailGate mit einem dieser MTAs zu kombinieren, sollte MailGate für „Standalone“ (also Relay-) Betrieb konfiguriert werden.

Beispielschemas für diese Konfiguration:

```
Internet → MailGate → Exim → weiterer MTA / Client (MUA)
```

```
Internet → MailGate → Exchange → Client (MUA)
```

3 MailGate Suite im Einsatz

3.1 Besonderheiten MailGate Suite

Die MailGate Suite kann als Lizenzupgrade zum normalen MailGate dazugekauft werden. Dabei handelt es sich technisch um dasselbe Produkt, wie MailGate. Es werden jedoch zusätzlich Funktionen über das Lizenzupgrade freigeschaltet.

Derzeit stellt die MailGate Suite eine zusätzliche AntiSpam Komplettlösung bereit.

Wenn Sie die MailGate Suite Funktionalität nutzen wollen, muss lediglich ein neues Keyfile eingespielt werden, dass die MailGate Suite beinhaltet. Darauf können Sie die AntiSpam-Optionen in der `/etc/avmailgate.conf` aktivieren.

Idealerweise wird die MailGate an der „Front“, also als erstes Bindeglied in der internen oder externen Mailinfrastruktur, genutzt.

Beispielschema für diese Konfiguration:

Internet → MailGate Suite → weiterer MTA / Client (MUA)

4 Praxisorientierte Tipps

4.1 Log-ging

Alle anfallenden Logdaten werden entweder ins Syslog, oder in eine gesonderte Logdatei geschrieben. Dabei gibt es hinsichtlich MailGate keine Überwachung, inwiefern die Logdatei eine Maximalgröße erreicht.

Dazu gibt es im Linux und UNIX-Umfeld seit langem Systemtools wie "logrotate", die einmal konfiguriert, Ihnen alle Arbeit abnehmen und anhand von eigenen Richtwerten automatisch rotieren.

4.2 Konfiguration

Im Folgenden können Sie von uns empfohlene erweiterte Einstellungen entnehmen:

MailGate (ohne AntiSpam)

/etc/avmailgate.conf:

MatchMailAddressForLocal	BOTH
LogFile	/var/log/avmailgate.log
MaxIncomingConnections	1024
ScanInArchive	YES
ArchiveMaxSize	128MB
ArchiveMaxRatio	150
ArchiveMaxRecursion	20
BlockSuspiciousArchive	YES
BlockUnsupportedArchive	YES
BlockEncryptedArchive	NO
BlockOnError	NO
ExposePostmasterAlerts	YES
ExposeRecipientAlerts	LOCAL
ExposeSenderAlerts	LOCAL
HeuristicsMacro	
HeuristicsLevel	3
DetectADSPY	yes
DetectAPPL	no
DetectBDC	yes
DetectDIAL	yes
DetectGAME	no

DetectHIDDENEXT	yes
DetectJOKE	no
DetectPCK	yes
DetectPHISH	yes
DetectSPR	no
AddXHeader	YES
AddReceivedByHeader	YES
OpenMax	2048

MailGate Suite (mit AntiSpam)

/etc/avmailgate.conf:

MatchMailAddressForLocal	BOTH
LogFile	/var/log/avmailgate.log
MaxIncomingConnections	1024
ScanInArchive	YES
ArchiveMaxSize	128MB
ArchiveMaxRatio	150
ArchiveMaxRecursion	20
BlockSuspiciousArchive	YES
BlockUnsupportedArchive	YES
BlockEncryptedArchive	NO
BlockOnError	NO
ExposePostmasterAlerts	YES
ExposeRecipientAlerts	LOCAL
ExposeSenderAlerts	LOCAL
HeuristicsMacro	
HeuristicsLevel	3
DetectADSPY	yes
DetectAPPL	no
DetectBDC	yes
DetectDIAL	yes
DetectGAME	no
DetectHIDDENEXT	yes
DetectJOKE	no
DetectPCK	yes
DetectPHISH	yes
DetectSPR	no
AddXHeader	YES
AddReceivedByHeader	YES



```
OpenMax                                2048

#
# Anti-Spam Konfiguration (MailGate Suite Lizenz nötig)
#
EnableSpamCheck                        YES

# Wichtige Optionen:
#
# SpamAction TAG:
#   ermöglicht ein benutzerabhängiges SpamFiltering,
#   entweder im Mail Client, oder in Ihrem Haupt-Mailserver
#
# SpamAction BLOCK:
#   führt zur sofortigen Quarantäne
#   Die Quarantäne kann über den AVQ-Manager ausgelesen und
#   verwaltet werden:
#
#   $ /usr/lib/AntiVir/avmailgate.bin --avq --help
#
SpamAction                             TAG

DangerousOutbreakAction                 BLOCK
DangerousAttachmentAction              TAG
DangerousAlertAction                   BLOCK
DangerousUnknownAction                  TAG

# Wichtig: Black- und White- Liste:
SpamFilterExceptions                    /etc/asmaligate.except

SpamFilterHandleBulkADVLikeSpam        NO
SpamFilterHandleBulkPornLikeSpam       YES
SpamFilterModifySubject                  YES
```

4.3 Updates

Um Ihre AntiVir Installation auf den aktuellen Stand zu halten, werden zwei Arten von Updates bei der Installation eingerichtet:

- Scannerupdate (nur Scanner & Engine & VDF)
- Produktupdate (MailGate Programmdateien)

Die Einstellungen für das Update finden Sie nach der Installation in folgender Datei:

/etc/cron.d/avira_updater:

```
36 */2 * * * root /usr/lib/AntiVir/avupdate --product=Scanner
39 11 * * Tue root /usr/lib/AntiVir/avupdate --
product=mailgate
```

Sinnvolle Werte für ein Update

Je nach Zielgruppe empfehlen wir unseren Kunden mindestens 2-3 mal am Tag, ein Update durchzuführen.

für große Unternehmen:

Beispiel: jede Stunde

/etc/cron.d/avira_updater:

```
* */1 * * * root /usr/lib/AntiVir/avupdate --product=Scanner
```

für Small Business:

Beispiel: alle 3 Stunden

/etc/cron.d/avira_updater:

```
* */3 * * * root /usr/lib/AntiVir/avupdate --product=Scanner
```

Kunden mit Schmalband Anschlüssen (Modem/ISDN):

Beispiel: alle 8 Stunden

/etc/cron.d/avira_updater:

```
* */8 * * * root /usr/lib/AntiVir/avupdate --product=Scanner
```

für ISPs

Für Internet Service Provider empfiehlt es sich natürlich, deutlich öfter nach neuen Signaturen zu schauen. Daher sollte die Frequentierung der Updateaufrufe deutlich höher angelegt sein, z.B. alle 15 Minuten. So ist sichergestellt, dass Sie immer zeitnah die neuesten Signaturen einsetzen.

/etc/cron.d/avira_updater:

```
*/15 * * * * root /usr/lib/AntiVir/avupdate --product=Scanner
```

Signaturenupdate

Es gibt darüber hinaus die Möglichkeit, ein reines Engine- und VDF- Update durchzuführen. Die MailGate Produkdateien, sowie der zentrale Scannerdienst (SAVAPI) werden dabei nicht mit aktualisiert.

Dies kann im Allgemeinen sehr interessant für Sie sein, wenn Sie Programmupdates als besonders sensitiv betrachten. Dadurch erhalten Sie die Möglichkeit, auf einem separaten Testsystem zunächst einen Audit durchzuführen, bevor Sie die neue Version produktiv einsetzen.

Der Aufruf dafür lautet:

```
$ /usr/lib/AntiVir/avupdate --product=Signatures
```