

# Release Notes zu GeNUGate 6.1

In diesen Release-Notes finden Sie Informationen zu der GeNUGate 6.1 Produktfamilie. Lesen Sie diese bitte aufmerksam durch! Wir empfehlen Ihnen unbedingt, dieses Upgrade zu installieren, da wir mit dieser Release nicht nur neue Features zur Verfügung stellen, sondern auch eine Reihe von Problemen behoben haben.

## Achtung!

Vor einem Upgrade empfehlen wir dringend, ein Konfigurations- oder besser noch ein vollständiges Backup der GeNUGate durchzuführen.

Eine ausführliche Anleitung zur Vorgehensweise beim Upgrade finden Sie im Kapitel 3 dieser Release Notes.

## Inhaltsverzeichnis

<b>1</b>	<b>Lieferumfang</b>	<b>2</b>
<b>2</b>	<b>Neuerungen in GeNUGate 6.1</b>	<b>2</b>
2.1	Sicherheitsfeatures . . . . .	2
2.2	Relays . . . . .	2
2.3	Mail . . . . .	5
2.4	HA . . . . .	5
2.5	VPN . . . . .	5
2.6	Sonstiges . . . . .	5
<b>3</b>	<b>Installation des Upgrades</b>	<b>7</b>
3.1	Upgradepfad . . . . .	7
3.2	Datensicherung . . . . .	7
3.3	Minimaler freier Festplattenspeicher . . . . .	7
3.4	Durchführung des Upgrades . . . . .	7
<b>4</b>	<b>So erreichen Sie uns</b>	<b>11</b>

## 1 Lieferumfang

Mit der neuen Version 6.1 der GeNUGate erhalten Sie:

- Diese Release Notes
- Eine bootfähige CD
- Eine gepackte PostScript- und PDF-Version des Handbuchs auf der GeNUGate-CD

## 2 Neuerungen in GeNUGate 6.1

### 2.1 Sicherheitsfeatures

- **Bind:** Der DNS Server Bind wurde auf the Version 9.3.4 aktualisiert. Die Sicherheitslücken CVE-2006-4095 bzw. VU#915404 und CVE-2006-4096 bzw. VU#697164 sind behoben.
- **Sendmail:** Der Mail-Transport-Agent sendmail wurde auf Version 8.13.8 aktualisiert.
- **Squid:** Der WWW-Cache Squid wurde auf Version 2.5.STABLE14 aktualisiert. Ausserdem wurden die Sicherheitslücken CVE-2007-247 und CVE-2007-248 behoben.
- **OpenSSH:** OpenSSH wurde auf die Version 4.5 aktualisiert.

### 2.2 Relays

- **Metarelays:** Zur einfacheren Bedienung wurden sog. „Metarelays“ implementiert, bei denen bereits zahlreiche Parameter voreingestellt sind. Diese sind wie konventionelle Relays in der Relay-Konfiguration auswählbar. Es sind die folgenden Meta-Relays definiert:

- ipsec
- ldap
- mssql
- mysql
- postgresql
- pptp
- rtsp
- snmptrap
- www-server

- **QoS:** Via GUI lässt sich der „Quality of Service“ für alle Relays ausser Telnet-Relay und FTP-Relay konfigurieren. Es wird sowohl der ältere Standard „Type of Service“ als auch das neuere „Differentiated Services Code Point“ unterstützt. Für letzteren werden die in RFC 2474 definierten „Class Selectors“ und die in RFC 2597 empfohlenen „Assured Forwarding“-Klassen angeboten.
- **SIP-Relay:** Ein neues Relay zur Unterstützung von Internettelefonie mit SIP (Session Initiation Protocol) und RTP (Real Time Protocol) ist in GeNUGate aufgenommen worden. Das Relay ist nur mit GeNUGate 200,400,600 und 800 und einem Paketfilter mit USB-Stick lauffähig.
- **RTSP-Proxy:** Zur Unterstützung des RTSP (Real-Time-Streaming Protocol) wurde ein neuer Dienst auf dem ALG implementiert. Für die einfache Benutzbarkeit wurde ein Meta-Relay namens „rtsp“ eingeführt, das ein tcprelay mit entsprechendem Mapping von Port 554 auf localhost:1554 definiert.
- **MAX\_CONNECT und FDs:** Die Limitierung von Filedescriptoren pro Relay und die Anzahl der maximal offenen Dateien im Kernel wurde erhöht. Für die Relays wurde zudem eine fein granulare Einstellung durch den Parameter MAX\_CONNECT realisiert.
- **SSLify WWW-Relay und TCP-Relay, Zertifikatsverwaltung:** In WWW-Relay und TCP-Relay wurde Unterstützung für SSL eingebaut. Es ist nun möglich, Verbindungen zwischen Client und Relay bzw. Relay und Server mit SSL zu verschlüsseln. Der „Bridge“-Modus erlaubt es einem Relay, den verschlüsselten Datenstrom zu inspizieren.

Für WWW-Relay und TCP-Relay existieren die Betriebsarten

- „Client-Relay-SSL“: Der Web-Browser kann sich mit SSL an das Relay verbinden und wird von dort unverschlüsselt zum Webserver weitergeleitet.
- „Bridging“: Der Datenstrom wird im Relay entschlüsselt, analysiert, wieder verschlüsselt und versandt. Um Warnungen des Browsers oder des SSL-Clients bezüglich falscher Zertifikate zu unterdrücken, muss die Certificate Authority der GeNUGate in den Client importiert werden.

Für TCP-Relay existiert die weitere Betriebsart „Relay-Server-SSL“, bei der die Verbindung zwischen TCP-Relay und Server mittels SSL gesichert wird.

Im GUI findet sich unter DIENSTE → SSL die X.509-Zertifikatsverwaltung zu den neuen Funktionen. Hier können Zertifikate erzeugt oder importiert werden um die neue SSL-Funktionalität von WWW-Relay oder TCP-Relay zu nutzen.

- **WWW-Relay:**
  - **https ohne squid:** Wird das WWW-Relay mit „Direkte Anfrage“ betrieben, so wurden alle HTTPS Requests bisher über den lokalen Squid-Proxy (127.0.0.1:8000)

weitergeleitet. Das ist jetzt nicht mehr notwendig, d.h. das WWW-Relay kann auch über HTTPS direkt mit dem Server ohne Zuhilfenahme eines Proxies kommunizieren.

- **Byte-Ranges/Windows-Updates:** Sogenannte „Range-Requests“ können von einem Browser abgesetzt werden, um bestimmte Teilbereiche einer Datei vom Web-Server anzufordern. Ist bei dem WWW-Relay der Virens Scanner konfiguriert, so werden solche Requests aus Sicherheitsgründen nicht erlaubt, da hierdurch Daten in Teilstücken empfangen und am Virens Scanner „vorbeigeschmuggelt“ werden können.

Wird eine URL oder ein Host explizit durch Angabe in der Scan-ACL vom Viren-Scannen ausgenommen, so sind die Range-Requests für diese URL/diesen Host erlaubt. Dadurch werden automatische Windows-Updates über ein derart konfiguriertes Relay erlaubt.

- **Ablösung von HTTP-Relay durch WWW-Relay:** Das HTTP-Relay dient zur Absicherung eines Web-Servers. Diese und weitere Funktionalität steht nun ebenfalls im WWW-Relay zur Verfügung. Zur einfacheren Konfiguration wurde ein Meta-Relay „WWW-Server“ definiert, welches auf WWW-Relay basiert.

Das HTTP-Relay wird mit einem der nächsten Releases nicht mehr unterstützt. Wir bitten Sie, bestehende HTTP-Relay Verbindungen auf das WWW-Relay umzustellen.

- **Squid:**

- **Löschen von URLs aus dem Squid-Cache:** Unter DIENSTE → WWW-CACHE → CACHE ENTLEEREN können im GUI nun einzelne URLs eingegeben werden, die aus dem Squid-Cache entfernt werden sollen. Um die Funktionalität benutzen zu können, muss die Methode PURGE manuell mittels einer Squid-ACL freigeschaltet werden. Geben sie hierzu im GUI unter DIENSTE → WWW-CACHE → KONFIGURATION für die entsprechende Squid Instanz in das Feld *ACL im Squid Format* folgendes ein:

```
acl PURGE method PURGE
http_access allow PURGE localhost
http_access deny PURGE
```

Um das Löschen des Squid-Caches durch normale Benutzer zu verbieten, muss im GUI unter DIENSTE → RELAYS für die Anfragemethoden ACL aller WWW-Relays

```
!PURGE *
```

eingetragen werden, so dass PURGE bereits durch das WWW-Relay verboten wird.

- **NTLM-Authentisierung:** Zusätzliche Programme wurden aufgenommen, die eine Authentisierung mittels NTLM am Squid erlauben. Hierzu müssen zahl-

reiche manuelle Einstellungen vorgenommen werden, die im Kundenbereich des GeNUA-Webservers beschrieben sind.

## 2.3 Mail

- **Meldungstexte konfigurieren:** Im GUI wurden unter DIENSTE → E-MAIL → FEHLERBEHANDLUNG die Einstellmöglichkeiten für Fehlertexte und das Verhalten des E-Mail-Systems im Fehlerfall verbessert.
- **DSN:** Die GeNUGate ist jetzt DSN-fähig, d.h. das Mail-Subsystem ist in der Lage, sogenannte Delivery Status Notifications nach Internet-Standard RFC 3461 zu verschicken. Das bedeutet, dass zu jeder vom GeNUGate ausgelieferten Mail im Fehlerfall detaillierte Benachrichtigungen in sowohl Menschen- als auch Maschinenlesbarem Format versendet werden. Die Art der Benachrichtigung kann im Rahmen des Standards vom ursprünglichen Absenders bei Bedarf noch durch Parameter im Maildialog gesetzt werden.

## 2.4 HA

- **EPING:** Ein GeNUGate HA-System kann mittels Ping-Paketen prüfen, ob der externe Router erreichbar ist. Dazu benötigt es permanente IP-Adressen am externen Interface. Werden diese und eine E-Ping Adresse im GUI konfiguriert, wird dieser Check des HA-Daemon jetzt aktiviert.

## 2.5 VPN

- **NAT-T:** Das VPN Modul benutzt jetzt RFC 3947 für IKE/IPsec NAT-Traversal. Damit ist VPN mit GeNULink verwendbar.

## 2.6 Sonstiges

- **Hardware-Überwachung:** GeNUGate 6.1 verfügt nun über die Möglichkeit diverse Parameter der Hardware zu überwachen. Wenn der Status einer der überwachten Hardwarekomponenten nicht mehr „OK“ ist, oder wenn der Wert den zulässigen Bereich überschreitet, kann z.b. dem Administrator eine E-Mail geschickt werden.

Bei der Installation oder einem Upgrade auf GeNUGate 6.1 werden die notwendigen Einstellungen automatisch vorgenommen, sofern die verwendete Hardware in der Liste der unterstützten Plattformen gefunden wird.

Wird die Hardware nicht automatisch erkannt, so muss der Administrator diese manuell im GUI unter SYSTEM → HARDWARE → KONFIGURATION → REVISION einstellen.

Passt keine der Voreinstellungen auf die von Ihnen verwendete Hardware, können Sie noch unter SYSTEM → HARDWARE → KONFIGURATION die erkannten Sensoren manuell einstellen.

- **cfgbu auf USB-Stick:** Mit GeNUGate 6.1 ist es nun möglich, ein Konfigurationsbackup auf einen – mit FAT32 formatierten – USB-Stick zu sichern.

```
# cfgbu -s -F /dev/sd2i
```

Je nach verwendeter Hardwareplattform muss der Name des Sticks als `/dev/sd0i` (GeNUGate 200) oder `/dev/sd2i` (GeNUGate 400,600,800) angegeben werden.

- **VLAN Support:** Im GUI können nun unter SYSTEM → INTERFACES VLAN Interfaces zu einem physikalischen Interface angelegt werden. Hierdurch ist es z.B. möglich, mehrere bisher physikalisch getrennte Interfaces des ALG zusammenzufassen und die physikalische Aufteilung der Datenpakete auf einem VLAN-fähigen Switch durchzuführen.
- **Support via ggsup/GUI:** Unter SYSTEM → SUPPORT → GGSUP besteht nun die Möglichkeit, Support Requests mit zahlreichen technischen Zusatzinformationen in Form einer verschlüsselten Mail an GeNUA zu senden.

Der Request kann auch als ZIP Datei auf einen z.B. Windows Rechner geladen werden, um die versandten Informationen zu überprüfen.

Wird durch das Formular eine Mail erzeugt, so ist diese stets mit dem GeNUA-Support-Key verschlüsselt, und kann nur von GeNUA entschlüsselt werden.

- **Recovery Installation:** Während der Installation kann nun ein Konfigurationsbackup von Diskette, USB-Stick oder einem SSH-Server eingespielt werden. Der SSH-Server kann auch ein HA-Partner sein.

Patches können während der Installation von USB-Stick, vom SSH-Server/HA-Partner und wie bisher auch vom GeNUA-Support-Server bezogen werden.

- **Änderung des Shell-Prompts:** Der Standard Shell-Prompt wird nun nach dem Schema `USER@HOST:/PATH$` gebildet, damit bei vielen offenen Terminal-Verbindungen eine bessere Übersicht gewährleistet ist.
- **Betriebsschlüssel:** Bei der Erkennung der Hardware kann es nach dem Upgrade durch einen Bugfix in Ausnahmefällen zu Meldungen wegen eines ungültigen Betriebsschlüssel geben.  
Wir bitten sie in diesen Fällen einen neuen Betriebsschlüssel über unseren Webserver anzufordern.

<https://support.genua.de/genugate/license/license.cgi>

## 3 Installation des Upgrades

### 3.1 Upgradepfad

**GeNUGates ab der Version 6.0 können auf die Version 6.1 aktualisiert werden.**

Ein bestimmtes Patchlevel der Version 6.0 ist hierbei nicht erforderlich.

### 3.2 Datensicherung

Im Gegensatz zum Upgrade von GeNUGate 5.1 auf GeNUGate 6.0 werden bei einem Upgrade auf GeNUGate 6.1 keine neuen Dateisysteme erzeugt. Logdateien und E-Mails im Spool-Verzeichnis bleiben also auf dem System erhalten.

Trotzdem sollten Sie vor dem Upgrade mittels

```
# cgbu -s
```

ein Backup ihrer Konfiguration durchführen.

Um ebenfalls E-Mails und Logdateien zu sichern muss ein Kompletbackup des Systems erstellt werden. Das Vorgehen hierzu ist im Handbuch, Kapitel 6.1 „Datensicherung“, beschrieben.

### 3.3 Minimaler freier Festplattenspeicher

Um den Upgrade erfolgreich durchzuführen, muss auf den verschiedenen Partitionen der Festplatte genügend freier Speicher vorhanden sein. Insbesondere sollten die Partitionen / und /usr mehr als 50% freien Speicherplatz haben.

### 3.4 Durchführung des Upgrades

Bitte beachten Sie:

**Sie benötigen zur Durchführung des Upgrade physikalischen Zugang zur GeNUGate oder eine serielle Konsole.**

Legen Sie die GeNUGate 6.1 CDRom in das Laufwerk, loggen Sie sich als Benutzer „admin“ auf das System ein und verwenden sie das Kommando `su` um „root“ zu werden.

```
$ su
Password:
Mar 14 13:06:33 ggd138 su: admin to root on /dev/console
#
```

Starten Sie `ggupgrade`, um das Upgrade zu starten.

```
# /usr/local/gg/sbin/ggupgrade
Starting GeNUGate Upgrade!
Starting /cdrom/usr/local/gg/sbin/ggupgrade ...
```

```

Vor dem Upgrade werden jetzt die Patches fuer das neue Release
geholt. Daher wird Ihr GeNUGate nach dem Upgrade gleich mit dem
aktuellsten Patchlevel arbeiten.

Before the upgrade the patches for the new release are fetched now.
That way your GeNUGate will start working with the latest patchlevel
right after upgrade.

Get upgrade patch from cdrom ...
Retrieving G610.000.tar
Extracting G610.000.tar

Die Patches fuer die neue Version können ueber das Internet von
GeNUA geholt werden.

The patches for the new version can be fetched from GeNUA over the
internet.

Patches von GeNUA (ja nein) [ja]? Patches from GeNUA (yes no) [yes]?

```

Sie können bereits vor dem Neustart des Systems nach veröffentlichten Patches suchen, wenn Sie hier *yes* oder *ja* eingeben.

Starten Sie nun das System neu.

```

# reboot
Mar 15 13:11:09 ggd138 reboot: rebooted by admin
/etc/rc.shutdown in progress...
IP is OFF
/etc/rc.shutdown complete.
Mar 15 13:11:12 ggd138 syslogd: exiting on signal 15
syncing disks... done
rebooting...

```

Achten Sie darauf, dass das System von der eingelegten GeNUGate 6.1 CD bootet. Dies wird durch den Text **CDBOOT 1.04** im Bootprompt bestätigt.

```

>> OpenBSD/i386 CDBOOT 1.04
boot>
booting cd0a:bsd.install: 4066920+776200 [52+213232+196563]=0x5028dc
entry point at 0x100120

[ using 410220 bytes of bsd ELF symbol table ]
Copyright (c) 1982, 1986, 1989, 1991, 1993
    The Regents of the University of California. All rights reserved.
Copyright (c) 1995-2006 OpenBSD. All rights reserved. http://www.OpenBSD.org

OpenBSD 3.9-stable (ALG.install) #0: Fri Mar  9 21:06:56 CET 2007
bluhm@g611.genua.de:/build/gg.61/61.D016/ALG.install
...

```

Nachdem der Kernel geladen ist, werden Sie von der GeNUGate 6.1 Installation begrüßt und müssen die Installationssprache und Tastaturbelegung auswählen. Bei der Auswahl des Installationsmodus wählen Sie *upgrade*.

```

GeNUGate Installation

Sprache auswaehlen.
Sprache/Language (de en) [de] ? [RETURN]

```

```
Belegung der an der GeNUGate angeschlossenen Tastatur auswaehlen.  
Tastaturbelegung (us de de.nodead ... pl hu si cf cf.nodead) [de.nodead] ? [RETURN]  
kbd: keyboard mapping set to de.nodead  
  
Systemerkennung.  
  
Installieren, Upgrade durchfuehren oder System vom Backup restaurieren.  
Modus (installation upgrade restaurieren) [installation] ? upgrade
```

Es werden nun die Festplatten geprüft und ins System eingebunden und für den Upgrade vorbereitet.

```
Festplatte mounten.  
Boot-Festplatte festlegen.  
Erkenne Festplatten im System.  
Boot-Festplatte erfolgreich festlegen.  
Alle Partition unmounten.  
Fstab auslesen.  
Dateisysteme ueberpruefen.  
/dev/rwd0a: file system is clean; not checking  
/dev/rwd0f: file system is clean; not checking  
/dev/rwd0d: file system is clean; not checking  
/dev/rwd0e: file system is clean; not checking  
Alle Partition mounten.  
Flags entfernen.  
GeNUGate Lizenzen.  
Lizenz initialisieren.
```

Die Lizenznummer und Hardware Seriennummer Ihres GeNUGate wird abgefragt. Die Werte aus GeNUGate 6.0 gelten weiterhin und Sie müssen nur *[RETURN]* drücken, um diese beizubehalten.

```
Lizenz eingeben.  
Der einzugebende Wert hat das Format 1234-GG-ABCD-EFGH-IJKL-MNOP.  
Lizenz [1234-GG-ABCD-EFGH-IJKL-MNOP] ? [RETURN]  
  
Seriennummer eingeben.  
Der einzugebende Wert hat das Format 1-234567.  
Seriennummer [1-234567] ? [RETURN]
```

Es besteht nun die Möglichkeit, Patches vom USB-Stick, vom HA-Peer oder via Netzwerk zu beziehen.

```
Patches vom USB-Stick holen.  
Patches vom USB-Medium holen (ja nein) [nein] ? [RETURN]  
  
Patches vom HA-Peer holen.  
Patches vom HA-Netzwerk holen (ja nein) [nein] ? [RETURN]  
  
Patches von GeNUA holen.  
Patches vom Netzwerk holen (ja nein) [nein] ? [RETURN]
```

Das Upgrade wird nun begonnen, die neue Software wird auf das System kopiert und die Konfiguration wird durchgeführt.

```
Upgrade beginnen.
```

```
Upgrade-Patch von Cdrom kopieren.
Retrieving G610_000.tar
...
```

Am Ende des Upgrade-Vorgangs werden Sie gefragt, ob Sie die Passwörter für den Administrator „admin“ und „root“ neu setzen wollen. Um die bestehenden Passwörter zu übernehmen, wählen Sie *nein* durch drücken von *[RETURN]*.

```
Administrator Passwoerter setzen.
Passwoerter setzen (ja nein) [nein] ? [RETURN]
```

Der Upgrade ist nun fertig. Drücken sie *[RETURN]* um das System neu zu starten und entfernen Sie die CD-ROM aus dem Laufwerk.

```
Druecken Sie <Return> zum Neustart und entfernen Sie nach der Meldung
'rebooting...' die CDRom aus dem Laufwerk.
Jetzt neu starten (neustart) [neustart] ? [RETURN]
```

Das System startet nun die neue Software. Nach dem Laden des Kernels werden Sie aufgefordert, das „root“ Passwort einzugeben, da noch ein Bootinstall-Skript für die Aktualisierung des Paketfilters ausgeführt werden muss.

```
Es wurde mindestens ein Bootinstall-Skript gefunden. Diese Skripten koennen
nur vom Systemverwalter ausgefuehrt werden. Daher wird jetzt nach dem
Passwort des Systemverwalters (root) gefragt. Wird das Passwort dreimal
falsch eingegeben, kann weiter gebootet werden, ohne dass die Bootskripten
ausgefuehrt wurden. Geben Sie bitte jetzt das root Passwort ein!
Sie haben 60 Sekunden sich zu authentisieren!

Root Passwort eingeben

Password:
```

Wählen Sie das Script aus der Liste durch *1* und *[RETURN]* führen Sie es durch Eingabe von *j* aus.

```
Waehlen Sie eine Liste von Boot Install Skripten aus, indem Sie die
entsprechenden Nummern eingeben, oder alle durch Eingabe von '*'
=====
1) /var/gg/boot/bootinst.2007.03.15-13.26.06.exe
   Paketfilter-Diskette Initialisieren

Auswahl (1) []: 1
1) /var/gg/boot/bootinst.2007.03.15-13.26.06.exe
   Paketfilter-Diskette Initialisieren
Ist das ok? (j/n) [n]: j
```

Stecken Sie die PFL-Diskette in das Laufwerk des ALG oder den PFL-USB-Stick in einen freien USB-Slot im ALG und schreiben das PFL Medium. Starten Sie den PFL gemäss den Anweisungen neu.

Wenn Sie sich nach Beendigung des Startvorgangs auf das ALG einloggen, werden Sie mit einer Meldung begrüsst, in der die neue Versionsnummer steht.

```
login: admin
Password:
Last login: Thu Mar 15 13:06:29 on console

        Welcome to your GeNUGate Firewall System.

        This system is running GeNUGate Version 6.1 000 based on OpenBSD 3.9

admin@ggd138:/var/home/admin$
```

Wir wünschen Ihnen viel Spass mit dem neuen System !

## 4 So erreichen Sie uns

GeNUA Gesellschaft für Netzwerk- und Unix-Administration mbH  
Domagkstraße 7, 85551 Kirchheim bei München,  
Tel. (089) 99 19 50-0, Fax. (089) 99 19 50-999  
E-Mail: [info@genua.de](mailto:info@genua.de), WWW: <http://www.genua.de/>

© 2007 GeNUA mbH, Kirchheim, Alle Rechte vorbehalten. GeNUGate und GeNUA sind eingetragene Warenzeichen der GeNUA mbH.