

GeNUBox 2.0 – Release-Notes

In diesen Release-Notes finden Sie Informationen zu der GeNUBox Version 2.0. Lesen Sie diese bitte aufmerksam durch! Wir empfehlen Ihnen dieses Upgrade zu installieren, da wir mit diesem Release nicht nur neue Features zur Verfügung stellen, sondern auch eine Reihe von Problemen beheben.

Inhaltsverzeichnis

1	Lieferumfang	1
2	Neuerungen GeNUBox	1
2.1	Aktualisiertes Betriebssystem	1
2.2	NAT-T Support	1
2.3	Redundant Network Access (RNA)	1
2.4	Dynamische IP-Adressen	1
2.5	GeNUBox-HA	1
2.6	Syslog Memory-Puffer-Support	2
2.7	SSHLD Durchsatz	2
2.8	Modem-Support	2
2.9	Dead Peer Detection (DPD)	2
3	Neuerungen Management-Server	3
3.1	Grafisches Monitoring	3
3.2	SSH Status-Anzeige	3
3.3	Flexiblere Wartung von GeNUBoxen	3
3.4	Verbessertes GUI	3
3.5	Bessere Zugriffskontrolle für SSH	3
3.6	Mehr Konsistenzchecks im GUI	3
3.7	Zeitzone-Auswahl	3
4	Interna und Fixes	4
4.1	IPsec VPN	4
4.2	Änderungen im Binärformat	4
4.3	Fehlerbehebung im TCP-Stack	4
5	Upgrade	5
5.1	Backup	5
5.2	Upgrade Management-Server	5
5.3	Upgrade Standalone-GeNUBox	6
6	So erreichen Sie uns	7

1 Lieferumfang

GeNUBox Management-Server Kunden erhalten:

- Diese Release Notes
- Eine autobootfähige CD mit:
 - der GeNUBox 2.0 Management Server Software (sowohl für Neuinstallation als auch für Upgrade)
 - dem GeNUBox 2.0 Standalone Upgrade Image
 - dem GeNUBox 2.0 Handbuch (PDF)

2 Neuerungen GeNUBox

2.1 Aktualisiertes Betriebssystem

Sowohl die GeNUBox, als auch der Management-Server basieren nun auf der aktuellen OpenBSD Version 3.6. (Siehe auch Punkt "Änderungen im Binärformat" unter "Internationale Fixes")

2.2 NAT-T Support

IPsec VPNs verfügen nun über NAT-T Support. Das bedeutet, dass IPsec VPNs auch über NAT-Router und UDP-Relays hinweg betrieben werden können.

2.3 Redundant Network Access (RNA)

Es ist nun möglich, eine redundante Anbindung an ein Netzwerk (z.B. Internet), zu realisieren. Dazu wird eine GeNUBox mit zwei Uplinks versorgt und jeweils ein Haupt- und ein Backup-Interface definiert. Dabei kann jegliche Kombination aus: Ethernet (z.B. Router), DSL (PPPoE) und Modem (über serielle Schnittstelle) benutzt werden.

2.4 Dynamische IP-Adressen

Es ist nun möglich einen Knoten eines IPsec VPNs mit einer dynamischen IP-Adresse zu betreiben.

2.5 GeNUBox-HA

Sie können nun zwei GeNUBoxen zu einem Hochverfügbarkeits-Verbund zusammenfügen.

Die bisher unterstützten Standardfälle sind:

- Router/Paketfilter
- SSH-Rendezvous-Server

- SSHLD-VPN Gateway
- IPsec-VPN Gateway

2.6 Syslog Memory-Puffer-Support

Der `syslogd` kann nun auf auf GeNUBoxen eingesetzt werden, welche nicht ständig via UDP mit einem Syslog-Server verbunden sind. Dazu loggt der `syslogd` in interne Memorybuffer. Diese können auf der Box mit dem Kommando `syslogc` ausgelesen werden.

2.7 SSHLD Durchsatz

SSHLD-VPNs erreichen durch eine Umstellung des Verschlüsselungs-Algorithmus (auf Blowfish) eine Durchsatz-Steigerung um ca. 25% (eine ausreichende Leitungskapazität vorausgesetzt).

2.8 Modem-Support

Die GeNUBox kann nun auch mit einem Modem an der zweiten seriellen Schnittstelle betrieben werden.

2.9 Dead Peer Detection (DPD)

Der für IPsec VPNs verwendete `isakmpd` verfügt nun über das in RFC 3706 definierte DPD Protokoll. Dies ermöglicht eine schnellere Ausfall-Erkennung von IPsec Partnern.

3 Neuerungen Management-Server

3.1 Grafisches Monitoring

Der Management-Server ermöglicht ein grafisches Monitoring der GeNUBoxen. Es werden RRD-Grafiken für Netzwerk-Durchsatz, CPU, Speicher und Paketfilter-Statistiken erstellt. Die Statistiken können in einer Granulation von Stunden bis hin zu Jahren dargestellt werden.

3.2 SSH Status-Anzeige

Der Management-Server ermöglicht nun die Status-Anzeige von aktiven SSH- und SSHLD-Verbindungen.

3.3 Flexiblere Wartung von GeNUBoxen

Konfigurationen, sowie die Box-Software lassen sich nun flexibler auf eine GeNUBox übertragen. Man kann optional eine andere IP-Adresse, einen Port, eine User/Passwort Kombination, sowie den automatischen Reboot konfigurieren.

3.4 Verbessertes GUI

Die neue GUI Startseite erlaubt nun die Auswahl der Datenbank und der Sprache (Deutsch oder Englisch).

Weiterhin verfügt das GUI nun über eine Session-Funktion, welche Teile der vom Nutzer gemachten Eingaben (z.B. Suchoptionen) vorhält.

Bei der Standortbeschreibung wurde ein Textfeld für beliebige Anmerkungen eingefügt.

3.5 Bessere Zugriffskontrolle für SSH

Der Zugriff auf den SSH-Dienst der GeNUBox lässt sich nun wahlweise auf Interfaces und Netzbereiche beschränken.

3.6 Mehr Konsistenzchecks im GUI

Das GUI warnt beim Löschen von Objekten (Boxen, Usern,...) falls diese noch an anderer Stelle als Referenz verwendet werden. Nach Bestätigung werden auch die Referenzen auf die gelöschten Objekte entfernt.

3.7 Zeitzone-Auswahl

Die Zeitzone der GeNUBox ist nun per GUI konfigurierbar.

4 Interna und Fixes

4.1 IPsec VPN

Die externen Interfaces einer GeNUBox werden nicht mehr als Teil eines IPsec VPN betrachtet. Das bedeutet, dass die direkte Kommunikation (z.B. Pings) zwischen IPsec Partnern nicht mehr verschlüsselt wird. Dadurch werden einige Kompatibilitätsprobleme mit VPN-Produkten diverser Fremdhersteller beseitigt.

4.2 Änderungen im Binärformat

Bedingt durch den Wechsel des Betriebssystems auf OpenBSD Version 3.6, wurde das Binärformat von *a.out* auf *ELF* gewechselt. Für bereits installierte Applikations-Pakete wird eine *a.out*-Emulation bereitgestellt. Prinzipiell sollten somit alte *a.out* Programme weiterhin funktionieren. Dennoch kann es besonders bei kernelnahen Anwendungen wie z.B. bei routing daemons zu Inkompatibilitäten kommen, welche eine Aktualisierung erfordern.

4.3 Fehlerbehebung im TCP-Stack

Ein Fehler im TCP-Stack ermöglichte es Angreifern durch das Senden von präparierten TCP-Timestamp-Optionen einen System Neustart (panic) auszulösen. Das Problem wurde behoben.

5 Upgrade

5.1 Backup

Vor einem Upgrade empfehlen wir dringend ein Backup Ihrer Konfigurationen, sowie der Datenbank des Management-Servers durchzuführen.

In Kapitel 2.3/S.14 des GeNUBox-Handbuchs Version 1.3 finden Sie eine detaillierte Anleitung, wie Sie das Backup vornehmen.

Folgende Verzeichnisse werden während des Upgrades komplett gelöscht! Sollten Sie irgendwelche wichtigen Dateien in einem dieser Verzeichnisbäume angelegt haben, bitten wir diese **vor** dem Upgrade entsprechend zu **sichern!**

```
/dev
/bin
/sbin
/var/postgresql
/var/packages
/var/db
/usr (mit Ausnahme von /usr/local/genubox/ext)
```

Es werden automatisch Backups der alten Version in folgenden Verzeichnissen angelegt:

```
/etc.1.3
/var/genubox/configs.1.3
/var/genubox/install.1.3
/usr/local/genubox/tftpboot.1.3
```

5.2 Upgrade Management-Server

Für den Upgrade muss der Management-Server mindestens den **Versionsstand 1.3** haben!

Das Upgrade-Skript übernimmt die wichtigsten Teile Ihrer bisherigen Konfiguration automatisch. Eventuelle Sonderanpassungen an Ihrem Management-Server können jedoch leider nicht berücksichtigt werden. Zu diesem Zweck finden Sie Ihre alten Konfigurationen unter `/etc.old`, welche Sie bei Bedarf von Hand zurückkopieren können.

Für den Upgrade gehen Sie bitte folgende Schritte durch:

- Loggen Sie sich als **root** auf dem Management-Server ein.
- Legen Sie die Upgrade-CD in das Laufwerk und mounten diese mittels:

```
# mount /dev/cd0c /mnt
```

- Starten sie das Upgrade-Skript mittels:

```
# sh /mnt/upgrade.sh
```

- Nachdem der erste Teil des Upgrades erfolgreich durchlaufen wurde, werden Sie aufgefordert, das System zu rebooten.
Drücken Sie dazu **ENTER**.
Bitte stellen Sie sicher, dass Ihr System von der eingelegten CD-ROM gebootet wird.
- Nach dem Booten von CD ist die Option 'U' (wie Upgrade) zu wählen.
- Die Upgrade-Routine versucht nun Ihre Root-Partition zu finden. Normalerweise sollten die vorgeschlagenen Default-Werte der darauf folgenden Fragen für Sie zutreffen. (Typischerweise: /wd0a/ , oder /sd0a/ bei SCSI-Systemen).
- Nach Beantwortung aller Fragen wird das System aktualisiert.
Bitte unterbrechen Sie diesen Vorgang nicht!
- Anschliessend werden Sie erneut zu einem Neustart aufgefordert. Entnehmen Sie die CD und booten Sie Ihr System wie gewohnt.
- Die letzten Schritte des Upgrades erfolgen automatisch beim Starten des Systems. Ihr System ist nun einsatzbereit.

Hinweis für Kunden mit manuellen Anpassungen des DHCP-Servers:

Unter Umständen müssen Ihre Änderungen händisch in der Datei install.cfg nachgetragen werden.

Lesen Sie dazu im Handbuch Abschnitt 2.2.4.

5.3 Upgrade Standalone-GeNUBox

Anmerkungen zu dem Upgrade:

Während des Upgrades wird eine Reihe zusätzlich benötigter Systemuser für spezielle Aufgaben Ihrer Konfiguration hinzugefügt. Diese geschützten User haben weder gültige Passwörter noch Homeverzeichnisse, und sind mit stark eingeschränkten Rechten versehen. Sie erhöhen die Systemsicherheit, indem Programme, die vorher unter dem User root ausgeführt wurden nur noch unter diesen geschützten User laufen (= "privilege separation").

Weiterhin wird die Datei syslog.conf um Einträge für das Logging in den Memory-Buffer ergänzt.

Für den Upgrade gehen Sie bitte folgende Schritte durch:

- Benutzen Sie einen Web Browser um zu der URL:
`https://support.genua.de/boximage/patches/patches.cgi`
zu gelangen.
- Geben Sie in dem Formular die Seriennummer Ihrer GeNUBox und 2.00 als GeNUBox Version ein. Klicken Sie auf "Patches anzeigen".
- Laden Sie die Datei B200.000.image.tgz herunter und speichern Sie diese.
- Loggen Sie sich als **root** auf der GeNUBox ein.
- Erzeugen Sie eine Upgrade-Partition mit den folgenden Befehlen:

```
# mkdir /var/upgrade
# mount_mfs -o rw -s 24500 swap /var/upgrade
```

- Kopieren Sie das neue Image auf Ihre GeNUBox:

```
# scp B200_000.image.tgz box:/var/upgrade
```

- Wechseln Sie in das Upgrade-Verzeichnis:

```
# cd /var/upgrade
```

- Prüfen Sie die Authentizität des Images mit:

```
# gzsig verify -v /etc/genua.pub B200_000.image.tgz
```

Die Ausgabe des obigen Kommandos sollte wie folgt lauten:

```
Verified B200_000.image.tgz
```

- Entpacken Sie das Image und starten Sie das Upgrade:

```
# tar xfvz B200_000.image.tgz
# sh updbox.sh
```

- Nachdem das Upgrade durchlaufen ist, können Sie die Box rebooten:

```
# reboot
```

- Update verifizieren: Nach dem Reboot können Sie das Update anhand der Ausgabe des folgenden Kommandos auf der GeNUBox verifizieren:

```
# cat /VERSION GeNUBox Version 2.0 (20.D008)
```

6 So erreichen Sie uns

GeNUA Gesellschaft für Netzwerk- und Unix-Administration mbH
Domagkstraße 7, 85551 Kirchheim bei München,
Tel. +49 (89) 99 19 50-0, Fax. +49 (89) 99 19 50-999
E-Mail: info@genua.de, WWW: <http://www.genua.de/>