

GeNUBox 2.0 – Release-Notes

These release notes contain important information to GeNUBox Version 2.0.

Please read carefully!

We recommend installing this upgrade, as not only a number of new features were added, but also several problems were fixed.

Contents

1	Delivery	1
2	What's New in GeNUBox 2.0	1
2.1	Updated Operating System	1
2.2	NAT-T Support	1
2.3	Redundant Network Access (RNA)	1
2.4	Dynamic IP Addresses	1
2.5	GeNUBox-HA	1
2.6	Syslog Memory Buffer Support	2
2.7	SSHLD Throughput	2
2.8	Modem Support	2
2.9	Dead Peer Detection (DPD)	2
3	Management Server: New Features	3
3.1	Graphical Monitoring	3
3.2	SSH Status Display	3
3.3	More Flexible Maintenance of GeNUBoxes	3
3.4	Improved GUI	3
3.5	Improved Access Control for SSH	3
3.6	More Consistency Checks in the GUI	3
3.7	Time Zone Selection	3
4	Internal Features and Fixes	4
4.1	IPsec VPN	4
4.2	Changed Binary Format	4
4.3	TCP Stack Fix	4
5	Upgrade	5
5.1	Backup	5
5.2	Management Server Upgrade	5
5.3	Upgrade of Standalone GeNUBox	6
6	Our Contact Data	7

1 Delivery

GeNUBox Management Server customers receive:

- These Release Notes
- An autoboot capable CD containing:
 - the GeNUBox 2.0 Management Server Software (both for new installation as well as for upgrade)
 - the GeNUBox 2.0 Standalone Upgrade Image
 - the GeNUBox 2.0 Manual (PDF)

2 What's New in GeNUBox 2.0

2.1 Updated Operating System

Both the GeNUBox and the Management Server now are based on the current OpenBSD version 3.6. (Compare section "Changed Binary Format" under "Internal Features and Fixes")

2.2 NAT-T Support

IPsec VPNs now include NAT-T support. This means that IPsec VPNs now also can connect via NAT routers and UDP relays.

2.3 Redundant Network Access (RNA)

Redundant connections to a network (e.g. the Internet) now are possible. To implement this, a GeNUBox contains two uplinks and has defined a main and a backup interface. Any combination of Ethernet (e.g. router), DSL (PPPoE) and modem (serial interface) can be used.

2.4 Dynamic IP Addresses

An IPsec VPN node now can be set up with a dynamic IP address.

2.5 GeNUBox-HA

Two GeNUBoxes can be combined to a HA cluster. The supported configurations are:

- Router/Paket filter
- SSH Rendezvous Server
- SSHLD-VPN Gateway
- IPsec-VPN Gateway

2.6 Syslog Memory Buffer Support

`syslogd` now can run on GeNUBoxes that are not constantly connected to a syslog server by UDP. Instead, `texttsyslogd` will log to internal memory buffers, which can be read with the command `syslogc`.

2.7 SSHLD Throughput

The encryption algorithm has been changed to blowfish, thus increasing the throughput of the SSHLD-VPNs by 25% (line capacity permitting).

2.8 Modem Support

GeNUBoxes now support a modem at the second serial interface.

2.9 Dead Peer Detection (DPD)

`isakmpd`, which is used for IPsec VPNs, now features the DPD protocol as described in RFC 3706. This speeds up the detection of failed or dead IPsec partners.

3 Management Server: New Features

3.1 Graphical Monitoring

The management server now performs graphical monitoring of GeNUBoxes. RRD graphs for network throughput, CPU, memory and packet filter statistics are displayed. All statistics can be displayed in a granulation of one hour up to years.

3.2 SSH Status Display

The management server now displays the status of active SSH and SSHLD connections.

3.3 More Flexible Maintenance of GeNUBoxes

The transfer of configuration files and box software to a GeNUBox now is far more flexible. New options are: configure a different IP address, port, user/password, and an automatic reboot.

3.4 Improved GUI

The new GUI start page now permits selection of database and language (German or English).

In addition, the GUI now has a session function which will store user entries (e.g. search options).

A free-form text field for arbitrary entries was added to the location description .

3.5 Improved Access Control for SSH

Access to the SSH service on the GeNUBox now can be limited to either interfaces or networks.

3.6 More Consistency Checks in the GUI

The GUI now warns if objects (boxes, users etc.) which still are referenced from elsewhere are deleted. If the deletion is confirmed, all references also are removed.

3.7 Time Zone Selection

The time on the GeNUBox now can be configured by the GUI.

4 Internal Features and Fixes

4.1 IPsec VPN

A GeNUBox's external interfaces no longer are seen as a part of an IPsec VPN. This means that direct communication between IPsec Partners (such as pings) no longer are encrypted. This eliminates compatibility problems with VPN products of various other manufacturers.

4.2 Changed Binary Format

Due to the changeover of the operating system to OpenBSD Version 3.6, the binary format has changed from *a.out* to *ELF*. An *a.out* emulation is provided for already installed application packages. Therefore, old *a.out* programs should continue to function. However, incompatibilities with certain lowlevel applications (e.g. routing daemons) are possible, and would require an update.

4.3 TCP Stack Fix

A bug in the TCP stack let attackers trigger a system restart (panic) by sending modified TCP timestamp options. The problem was fixed.

5 Upgrade

5.1 Backup

Prior to an upgrade we strongly recommend performing a backup of your current configuration and the management server's database.

Detailed instructions for carrying out an upgrade are available in chapter 2.3/page 14 of the GeNUBox version **1.3** manual.

The following directories are deleted during upgrade! If any important files were created in these paths, please perform a **backup before the upgrade!**

```
/dev
/bin
/sbin
/var/postgresql
/var/packages
/var/db
/usr (except for /usr/local/genubox/ext)
```

The following backup directories are automatically generated, and the old directory versions copied to them:

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

5.2 Management Server Upgrade

To be upgraded, the management server must at least be at **version 1.3!** The upgrade script will automatically handle most of your configuration tasks. Individual adjustments however must be done manually - please check your old configuration under `/etc.old` if you wish to restore selected files.

Please carry out the following steps during upgrade:

- Log on the management server as **root**.
- Put the upgrade CD in the drive and mount it:

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

- Start the upgrade script:

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

- After the first part of the upgrade was successfully completed you are prompted to reboot the system.
Press **ENTER** to do so.
Please make sure your system is booted from the inserted CD.

- After booting from CD, choose the option 'U' (as in Upgrade).
- The upgrade routine now tries to find the system's root partition. In most cases, the suggested default answers to the following questions should apply to the system (typically: /wd0a/, or /sd0a/ for SCSI systems).
- After answering all questions the system is upgraded.
Do not interrupt this process!
- You again are prompted to reboot - remove the CD and boot the system as usual.
- The last upgrade steps are automatically performed during the system's startup. Your system now is ready.

Note for customers with manually configured DHCP servers:

Your modifications may have to be manually added to the file install.cfg . Please check the manual, section 2.2.4.

5.3 Upgrade of Standalone GeNUBox

Upgrade Notes:

A number of necessary system users for special functions will be added to your configuration during upgrade. These protected users have neither valid passwords nor home directories, and only greatly restricted permissions. They are used to increase system security by running programs formerly executed by root (= "privilege separation").

In addition, entries for logging in memory buffers will be added to the file syslog.conf. Please carry out the following steps during upgrade:

- Use a web browser and enter the URL:
`https://support.genua.de/boximage/patches/patches.cgi`
- Enter your GeNUBox's serial number and 2.00 as the GeNUBox version. Click on "ShowPatches".
- Download and save the file B200_000.image.tgz .
- Log on to the GeNUBox as root.
- Create an upgrade partition:

```
# mkdir /var/upgrade  
# mount_mfs -o rw -s 24500 swap /var/upgrade
```
- Copy the new image to your GeNUBox:

```
# scp B200_000.image.tgz box:/var/upgrade
```
- Change to the upgrade directory:

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

- Verify the image's authenticity:

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

The output of the command above should be:

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

- Unpack the image and start the upgrade:

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

- After the upgrade has finished, reboot the box:

```
# reboot
```

- Verify update: After reboot you can verify the update with the following commands on the GeNUBox:

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

6 Our Contact Data

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/>