

# Release Notes zu GeNUCenter

## 1.1

In diesen Release-Notes finden Sie Informationen zu GeNUCenter 1.1 . 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-Backup des GeNUCenter durchzuführen.

Eine ausführliche Anleitung zur Vorgehensweise beim Upgrade finden Sie im Abschnitt 5 dieser Release Notes.

### Inhaltsverzeichnis

<b>1</b>	<b>Lieferumfang</b>	<b>2</b>
<b>2</b>	<b>Neuerungen in GeNUCenter 1.1</b>	<b>2</b>
2.1	Betriebssystem-Update . . . . .	2
2.2	GUI Verbesserungen . . . . .	2
2.3	GeNUGate Verwaltung . . . . .	3
2.4	Organisation teilvermaschter VPN Topologien . . . . .	3
2.5	Logging . . . . .	3
2.6	Ausfallsicheres GeNUCenter . . . . .	4
<b>3</b>	<b>Geänderte Funktionalität</b>	<b>4</b>
3.1	Negierte Quellen und Ziele in Filterregeln . . . . .	4
<b>4</b>	<b>Neuerungen für GeNUScreen und GeNUCrypt</b>	<b>4</b>
4.1	Performance Verbesserungen . . . . .	4
4.2	Hochverfügbarkeit . . . . .	5
4.3	Filter . . . . .	5
<b>5</b>	<b>Installation des Upgrades</b>	<b>5</b>
<b>6</b>	<b>So erreichen Sie uns</b>	<b>7</b>

## 1 Lieferumfang

Mit der neuen Version 1.1 von GeNUCenter erhalten Sie:

- Diese Release Notes
- Eine bootfähige CD-ROM

## 2 Neuerungen in GeNUCenter 1.1

### 2.1 Betriebssystem-Update

Das als Basis des Produkts verwendete Betriebssystem OpenBSD wurde auf die Version 4.1 aktualisiert. Eine ausführliche Liste der Änderungen finden Sie auf

<http://www.openbsd.org/plus40.html>

und

<http://www.openbsd.org/plus41.html>

### 2.2 GUI Verbesserungen

Die GeNUCenter GUI wurde grundlegend überarbeitet und erheblich verbessert:

- Inline-Editieren: es ist jetzt möglich, referenzierte Definitionen in Dialogen anzulegen und zu editieren. Zum Beispiel können in der Definition einer Filterregel neue Netze und Dienste definiert werden.
- Elemente einer Seite werden per Javascript bei Bedarf vom GeNUCenter bezogen, ohne dass die ganze Seite neu geladen werden muss. Zum Beispiel kann die Online-Hilfe ein- und ausgeblendet werden, ohne dass bereits vorgenommene, noch nicht ausdrücklich abgespeicherte Eingaben verloren gehen.
- Landkarten: Eine neue Übersichtsseite erlaubt Ihnen, die verwalteten Appliances auf Landkarten zu positionieren; der Zustand der Appliances wird auf der Karte angezeigt und alle fünf Minuten automatisch auf den neuesten Stand gebracht.
- Dienste für Filterregeln können beliebig gruppiert werden. Beispielsweise können alle IPsec-relevanten IP Protokolle und UDP Dienste zu einem zusammengefasst werden, so dass nur eine Filterregel definiert werden muss.
- Filterregeln können nun mit Kommentaren versehen werden.
- Subdomains: Appliances können nun in Gruppen — *Subdomains* — eingeteilt werden, die sich gemeinsame Definitionen teilen. Administratoren können angelegt werden, deren Autorität sich auf einzelne Subdomains beschränkt.

- Bulk Actions: Mehreren ausgewählten Appliances einer Subdomain können gleichzeitig Filterregeln oder VPN Partner zugewiesen werden. Dadurch wird die Administration einer großen Anzahl von Maschinen vereinfacht.
- Tagging: Beliebige Objekte können mit "Tags" versehen werden. In den Übersichtsseiten kann danach gesucht werden.
- Suche: Alle verwaltete Objekte können nach Begriffen und Netzen durchsucht werden. Dadurch wird die Administration zahlreicher Appliances mit vielen Filterregeln und Netzdefinitionen erleichtert.

### 2.3 GeNUGate Verwaltung

Mit der neuen Version ist es jetzt möglich, schon vorinstallierte GeNUGates (ab Version 6.2 Patch 1) mit dem GeNUCenter zu verwalten.

- Komfortable und übersichtliche Verwaltung von Relays
- Mehrere Relay Definitionen können sich Quell-, Ziel- und Listener teilen
- Logs, Reports und Accounting Daten werden zentral gesammelt
- Konfigurations Backups können auf dem GeNUCenter gesammelt werden
- Updates können vom GeNUCenter Management Server auf GeNUGates eingespielt werden (erfordert allerdings Eingriff vor Ort)

### 2.4 Organisation teilvermaschter VPN Topologien

Es ist jetzt möglich, bei komplexeren VPN Topologien eine Appliance als zentralen *Hub* einer sternförmigen VPN Verbindungsgruppe zu konfigurieren. Die Appliances mit VPN Verbindungen zum Hub können untereinander durch den Hub hindurch kommunizieren. Der Hub sieht den Datenstrom im Klartext, kann also noch Filterregeln anwenden.

### 2.5 Logging

Das Logging wurde erheblich erweitert.

- Gezieltes Durchsuchen von Logdaten. Insbesondere können Logdaten zu Filtervorgängen nach IP Adressen oder Netzen durchsucht werden.
- Graphische statistische Auswertungen über wählbare Zeitabschnitte
- Es werden auch Statistiken über das GeNUCenter selbst erzeugt. Unterem anderem wird die Plattenauslastung angezeigt.
- Reports: Berichte im PDF Format über Verbindungsdaten, Anwendung von Filterregeln etc. können pro Appliance über verschiedene Zeitspannen erzeugt werden.

- Es können Accountingdaten pro Verbindung erzeugt werden. Damit können über Filterregeln Quelle, Ziel und Datenvolumen pro einzelner TCP oder UDP Verbindung aufgezeichnet werden.

## 2.6 Ausfallsicheres GeNUCenter

Das Center selbst kann jetzt ausfallsicher betrieben werden. Eine zweite Maschine wird als GeNUCenter installiert und im ersten als Slave registriert.

## 3 Geänderte Funktionalität

Der Upgrade bringt eine Änderung mit sich, die unter Umständen Anpassungen Ihrer Konfiguration erfordert.

### 3.1 Negierte Quellen und Ziele in Filterregeln

In GeNUCenter 1.0 war es möglich, Regeln auf "verneinte" Quellen und Ziele anwenden zu lassen. Die Funktionalität ist durch das Upgrade in die Netzwerk Definitionen verschoben worden, damit sie leichter in anderen Regeln genutzt werden kann.

Sollten Sie auf Ihrem GeNUCenter Regeln definiert haben, die solche Quell- oder Zielnetze verwenden, werden Sie beim Upgradevorgang, wie unten beschrieben, gewarnt. Das Upgradeprogramm zeigt Ihnen eine Liste von URLs an, mit denen Sie direkt zu den betreffenden Regeln gelangen können.

Um eine solche Regel anzupassen, definieren Sie ein Netzwerk Objekt, in dem die betreffenden Ziel- oder Quelladressen verneint sind, und fügen Sie zusätzlich — ohne Verneinung — das Netz 0.0.0.0/0 hinzu. Verwenden Sie dieses Netzwerk Objekt dann als Quelle oder Ziel Ihrer Filterregel. Wenn Sie negierte Schnittstellen als Quelle oder Ziel verwendet haben, müssen Sie alle Adressen der betreffenden Schnittstelle in die Netzwerkdefinition übernehmen.

## 4 Neuerungen für GeNUScreen und GeNUCrypt

Der Upgrade bringt auch für die verwalteten Appliances neue Features und Verbesserungen.

### 4.1 Performance Verbesserungen

An vielen Stellen wurde die Performance verbessert und Techniken für besseren Skalierung eingeführt.

- Schnelleres Filtern : Die Filterfunktionen sind jetzt schneller; auf der kompakten 100C Hardware, Revision 2 und 3, kann nun mit in etwa doppelter Geschwindigkeit gefiltert werden.
- Schnelleres VPN : Auf der 100C Revision 3 Hardware mit VIA C7 Prozessor sind VPN Verbindungen wesentlich beschleunigt worden, in dem die prozessorinternen Kryptofunktionen benutzt werden.

## 4.2 Hochverfügbarkeit

- `trunk` Schnittstellen: Es können auf GeNUScreen mehrere Ethernet Schnittstellen zu `trunk` Schnittstellen gebündelt werden. Wenn die Verkabelung über verschiedene Switches geht, kann so Ausfallsicherheit auf Layer 2 erreicht werden.

## 4.3 Filter

Die GeNUScreen Filterfunktionen wurden erweitert und die GUI verbessert.

- Feineres Filtern von VPN: VPN-Datenverkehr kann jetzt feingranularer gefiltert werden. Es können jetzt VPN-Partner als Quell- und Ziel-Interfaces in Filterregeln verwendet werden.
- Vordefinierte Dienste: Es wurden Dienste für zahlreiche übliche Protokolle vordefiniert.
- Accounting pro Verbindung: Verbindungsdauer, Quelle, Ziel und Datenvolumen einzelner Verbindungen können geloggt werden.
- *NetFlow*<sup>TM</sup> Support: GeNUScreen kann jetzt die gesammelten Logs zu Verbindungen über das *NetFlow*<sup>TM</sup> Protokoll (Versionen 1 und 5) an einen Collector schicken.
- Live-Anzeige von Filterzuständen: Die GUI zeigt jetzt alle aktuell bestehenden Verbindungen an. Aus dieser Übersicht ist es möglich, die zugehörige Filterregel direkt einzusehen und zu editieren, als auch einzelne Verbindungen gezielt abzurechnen.
- Mehrere Quell- und Zieladressen pro Regel: Es können jetzt mehrere Quell- und Zieladressen in einer Regeldefinition eingetragen werden.
- Kombinierte TCP und UDP Dienste: Dienste für Filterregeln können gruppiert werden. Beispielsweise können die Services für TCP und UDP Port 53 zu einem DNS Services zusammengefasst werden.

## 5 Installation des Upgrades

Für den Upgrade des GeNUCenters wird als Ausgangspunkt ein Versionsstand von GeNUCenter 1.0p5 empfohlen.

Der Upgrade stellt sich als Neuinstallation des GeNUCenters mit anschließendem Einspielen eines Datenbank Backups dar. Dadurch haben Sie die Möglichkeit, nach dem Einspielen der Datenbank das Ergebnis über das Webinterface zu kontrollieren, bevor Sie die Konfiguration aktivieren.

Zur Vorbereitung des Upgrades kontrollieren Sie bitte, ob Sie einen SSH-Zugang zum GeNUCenter haben, und richten diesen gegebenenfalls ein.

Für den Upgrade gehen Sie bitte folgende Schritte durch:

- Loggen Sie sich als `root` auf Ihrem GeNUCenter ein.

- Erstellen des Datenbank Backups:

Führen Sie dazu folgendes Kommando aus:

```
$ db_backup -f /var/tmp/upgrade_config_backup.dbak center_production
```

Analog dazu lassen sich die Logdaten sichern:

```
$ db_backup -f /var/tmp/upgrade_logging_backup.dbak logging_center_production
```

- Kopieren Sie die beiden Dateien

```
/var/tmp/upgrade_config_backup.dbak
```

und

```
/var/tmp/upgrade_logging_backup.dbak
```

auf einen anderen Rechner (z.B. mit `scp`).

- Installieren Sie nun Ihr GeNUCenter System mit der neuen Version.
- Loggen Sie sich über das Webinterface ein und richten Sie sich einen SSH-Zugang ein. (Achten Sie dabei auf die SSH-ACL.)
- Kopieren Sie die beiden oben gesicherten Datenbank Backups auf Ihr GeNUCenter nach `/var/tmp`.
- Spielen Sie die Backups wieder ein:

```
$ db_restore -d logging_center_production /var/tmp/upgrade_logging_backup.dbak
```

```
$ db_restore -d center_production /var/tmp/upgrade_config_backup.dbak
```

In diesem Schritt wird die Datenbank auf die neue Version migriert. Dabei werden einige Tests durchgeführt. Bitte achten Sie auf eventuelle Warnungen am Ende der Ausgaben. Unter Umständen kann es vorkommen, daß Sie gebeten werden, einzelne Teile Ihrer Konfiguration im GUI auf ihre Semantik hin zu überprüfen. Die nötigen Schritte sind in Abschnitt 3 erklärt.

- Jetzt können Sie sich am Webinterface anmelden und das Ergebnis kontrollieren. Es wird empfohlen, zumindest die Konfiguration des GeNUCenter selbst zu kontrollieren um bei aufgetretenen Fehlern nach Aktivieren der Konfiguration nicht den Kontakt zu diesem zu verlieren.

- Aktivieren Sie nun die Konfiguration des GeNUCenters über die Wartungsfläche im Webinterface.

## 6 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/>