Raspberry – Ntopng Traffic Server

Vorbereitung:

Das Raspbian OS Bullseye Lite 64Bit mit dem Raspberry Pi Imager auf eine SD- Karte schreiben.
Danach den Raspberry hochfahren und mit dem IP-Scanner die IP-Adresse herausfinden.
Mit der IP-Adresse über den Putty verbinden.

```
mario@raspberrypi:~ $ sudo apt-get update && sudo apt-get full-upgrade -y
Get:1 http://security.debian.org/debian-security bullseye-security InRelease [27.2 kB]
Hit:2 http://deb.debian.org/debian bullseye InRelease
Get:3 http://deb.debian.org/debian bullseye-updates InRelease [44.1 kB]
Get:4 http://archive.raspberrypi.org/debian bullseye InRelease [39.0 kB]
Get:5 http://security.debian.org/debian-security bullseye-security/main arm64 Packages [339 kB]
Get:6 http://security.debian.org/debian-security bullseye-security/main armhf Packages [336 kB]
```

Mit diesem Befehl den Raspberry updaten. Danach mit sudo reboot neustarten.

Installation Ntopng:

```
mario@raspberrypi:~ $ wget https://packages.ntop.org/RaspberryPI/apt-ntop.deb
--2025-02-10 09:54:24--  https://packages.ntop.org/RaspberryPI/apt-ntop.deb
Resolving packages.ntop.org (packages.ntop.org)... 167.99.215.164, 2a03:b0c0:2:d0::d27:3001
Connecting to packages.ntop.org (packages.ntop.org)|167.99.215.164|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3226 (3.2K) [application/vnd.debian.binary-package]
Saving to: 'apt-ntop.deb'

apt-ntop.deb                        100%[=============================================================================================>]   3.15K  --.-KB/s    in 0s

2025-02-10 09:54:24 (27.2 MB/s) - 'apt-ntop.deb' saved [3226/3226]
```

Mit diesem Befehl wird das Installationspaket heruntergeladen.

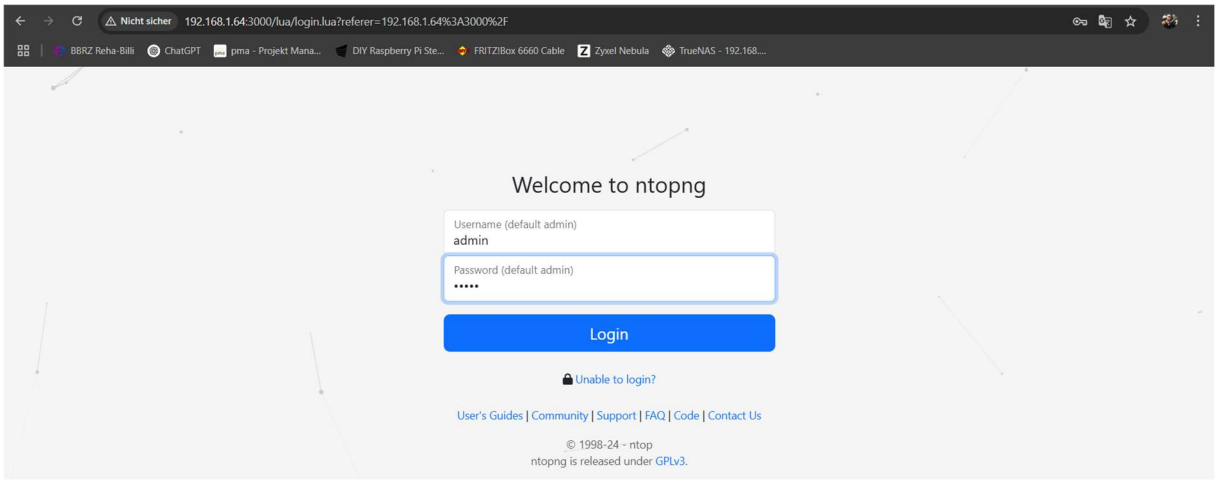
```
mario@raspberrypi:~ $ sudo dpkg -i apt-ntop.deb
Selecting previously unselected package apt-ntop.
(Reading database ... 37780 files and directories currently installed.)
Preparing to unpack apt-ntop.deb ...
Unpacking apt-ntop (2.9-16) ...
Setting up apt-ntop (2.9-16) ...
Installing ntop GPG key. Please wait...
gpg: keybox '/usr/share/keyrings/ntop-archive-keyring.gpg' created
gpg: /root/.gnupg/trustdb.gpg: trustdb created
gpg: key 3D84C955924F7599: public key "Luca Deri <deri@ntop.org>" imported
gpg: Total number processed: 1
gpg:               imported: 1
```

Mit diesem Befehl wird die Datei „apt-ntop.deb“ mit dem Debian-Paketmanager installiert. Danach mit „sudo apt-get update“ eventuelle fehlende Pakete installieren.

```
mario@raspberrypi:~ $ sudo apt-get install ntopng nprobe
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  bridge-utils fontconfig libcairo2 libdatriel libdbi1 libfribidi0 libgraphite2-3 libharfbuzz0b libhiredis0.14 libjemalloc2 liblinear4 liblua5.1-0 liblua5.3-0 liblzf1 libmariadb3
  libnetfilter-queue1 libnorm1 libnuma1 libpango-1.0-0 libpangocairo-1.0-0 libpangoft2-1.0-0 libpgm-5.3-0 libpixman-1-0 libradcli4 librdkafka1 librrd8 libsensors-config libsensors5
  libsnmp-base libsnmp40 libsodium23 libthai-data libthai0 libxcb-render0 libxcb-shm0 libxrender1 libzmq5 lua-bitop lua-cjson lua-lpeg mariadb-common mysql-common ndpi nmap nmap-common
  ntopng-data redis-server redis-tools
Suggested packages:
  liblinear-tools liblinear-dev lm-sensors snmp-mibs-downloader ncat ndiff zenmap ruby-redis
```

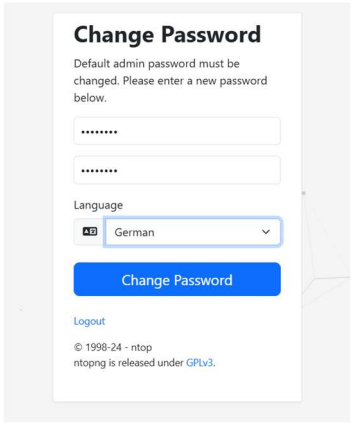
Mit diesem Befehl werden die Pakete „ntopng“ und „nprobe“ über den APT-Paketmanager installiert.

Ntopng Erstanmeldung und Einrichtung:

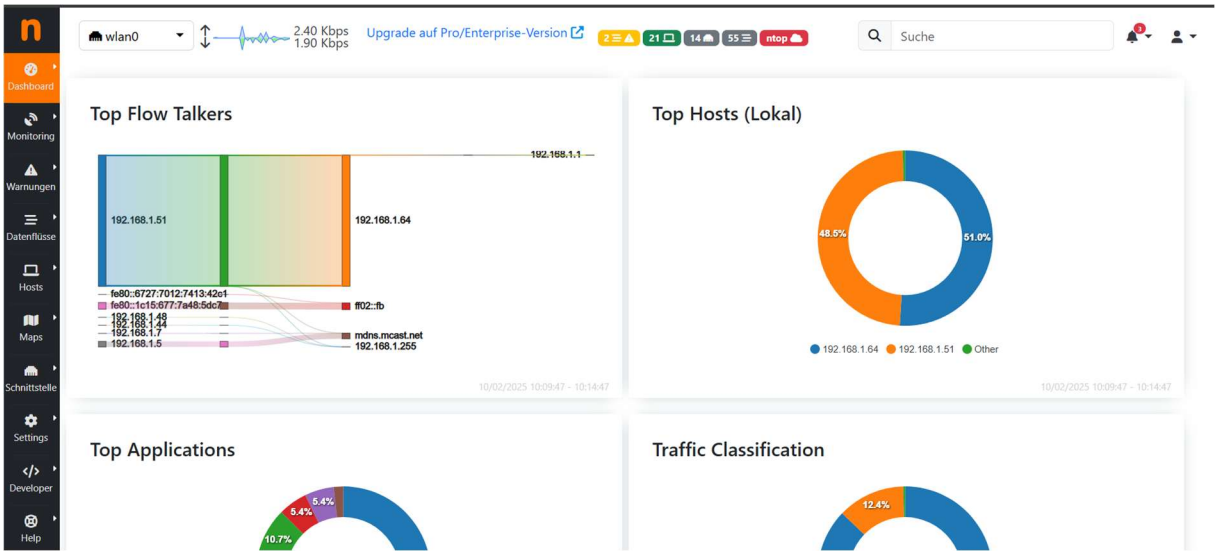


Mit der IP-Adresse des Raspberry´s und dem Port 3000 kommt man auf die WebGui-Oberfläche.

Bei der Erstanmeldung ist der Username + Passwort „admin“.



Nach der Erstanmeldung wird die Änderung des Passworts verlangt. Es können hier auch Spracheinstellungen getätigt werden.



Nach der Anmeldung kommt man zum Dashboard. Von dieser WebGui können jetzt Alarme sowie Datenflussaufzeichnungen eingestellt werden.

Zusammenfassung:

Ntopng ist ein leistungsstarkes, web-basiertes Netzüberwachungs- und Analyse-Tool. Es bietet Echtzeit-Überwachung des Netzwerkverkehrs und hilft Administratoren, die Bandbreitennutzung, Netzwerkleistung und potenzielle Sicherheitsrisiken zu analysieren.

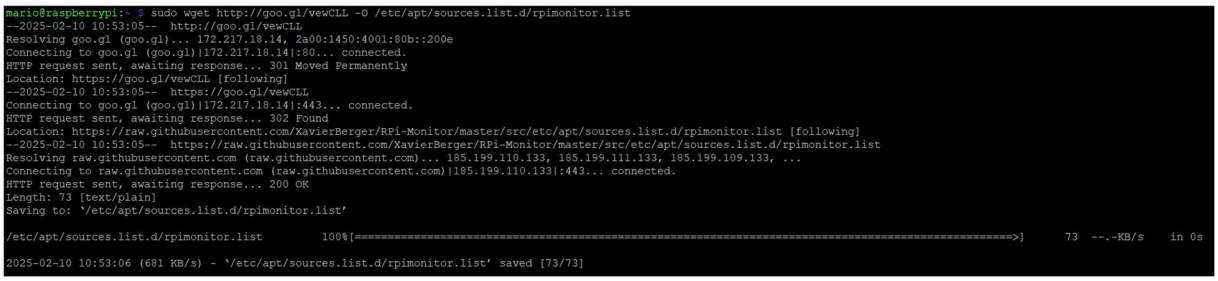
Wichtige Funktionen:

- **Echtzeit-Netzwerküberwachung:** Zeigt Verkehrsdaten, aktive Hosts und deren Kommunikationsverhalten an.
- **Detaillierte Traffic-Analyse:** Erkennt Protokolle wie HTTP, HTTPS, DNS, VoIP und zeigt deren Nutzung.
- **Flow-basierte Analyse:** Unterstützt NetFlow, sFlow und IPFIX zur detaillierten Traffic-Untersuchung.
- **Host- und Geräte-Erkennung:** Zeigt verbundene Geräte und deren Datenverkehr.
- **Sicherheitsüberwachung:** Erkennt verdächtigen Datenverkehr und mögliche Angriffe.
- **Web-Oberfläche:** Intuitive Darstellung der Netzwerkaktivitäten über einen Browser.
- **Integration mit anderen Tools:** Funktioniert mit nProbe, ElasticSearch, Grafana und Prometheus.

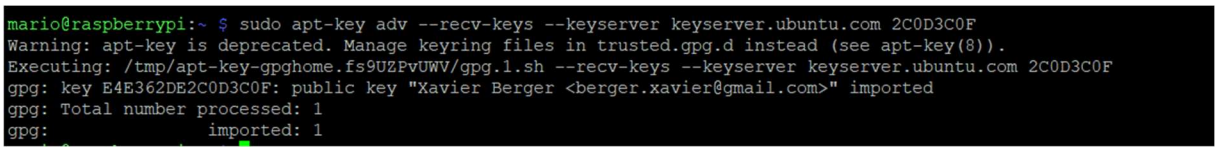
Einsatzbereiche:

- Netzwerk-Fehlersuche und Performance-Analyse
- Sicherheitsüberwachung und Bedrohungserkennung
- Bandbreitenmanagement und Nutzungsanalyse

Installation RPi Monitor:



Mit diesem Befehl wird das Installationspaket heruntergeladen.



Dieser Befehl wird verwendet, um einen GPG-Schlüssel zu einem Debian- oder Ubuntu-System hinzuzufügen. Dieser Schlüssel wird benötigt, um Pakete aus einer bestimmten Paketquelle zu verifizieren.

```
mario@raspberrypi:~ $ sudo apt-get update
Hit:1 http://deb.debian.org/debian bullseye InRelease
Get:2 http://deb.debian.org/debian bullseye-updates InRelease [44.1 kB]
Hit:3 http://security.debian.org/debian-security bullseye-security InRelease
Hit:4 http://archive.raspberrypi.org/debian bullseye InRelease
Get:5 http://giteduberger.fr rpimonitor/ InRelease [1,933 B]
Hit:6 https://packages.ntop.org/apt/bullseye_pi arm64/ InRelease
Hit:7 https://packages.ntop.org/apt/bullseye_pi all/ InRelease
Get:8 http://giteduberger.fr rpimonitor/ Packages [359 B]
Fetched 46.4 kB in 2s (27.5 kB/s)
Reading package lists... Done
```

Mit diesem Befehl werden wieder fehlende Pakete geholt.

```
mario@raspberrypi:~ $ sudo apt-get install rpimonitor
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  aptitude aptitude-common libboost-iostreams1.74.0 libclone-perl libcommon-sense-perl libcwidget4 libencode-locale-perl libfile-which-perl libhttp-daemon-perl libhttp-date-perl
  libhttp-message-perl libio-html-perl libipc-sharelite-perl libjson-perl libjson-xs-perl liblwp-mediatypes-perl librrds-perl libsigc++-2.0-0v5 libtimedate-perl libtypes-serialiser-perl
  liburi-perl libxapian30
Suggested packages:
  apt-xapian-index aptitude-doc-en | aptitude-doc debtags libcwidget-dev libwww-perl xapian-tools
The following NEW packages will be installed:
  aptitude aptitude-common libboost-iostreams1.74.0 libclone-perl libcommon-sense-perl libcwidget4 libencode-locale-perl libfile-which-perl libhttp-daemon-perl libhttp-date-perl
  libhttp-message-perl libio-html-perl libipc-sharelite-perl libjson-perl libjson-xs-perl liblwp-mediatypes-perl librrds-perl libsigc++-2.0-0v5 libtimedate-perl libtypes-serialiser-perl
  liburi-perl libxapian30 rpimonitor
0 upgraded, 23 newly installed, 0 to remove and 0 not upgraded.
```

Mit diesem Befehl wird der RPI-Monitor installiert.

```
mario@raspberrypi:~ $ sudo /etc/init.d/rpimonitor update
RPi-Monitor update packages status:.
```

Mit diesem Befehl wird bewirkt, dass Informationen über upgradebare Pakete aktualisiert werden.

Danach sollte das System neugestartet werden. Der Monitor ist nun im Browser unter der IP-Adresse des Raspberry und dem Port 8888 erreichbar.