



Lösung: kein ipv4, kein portforwarding, kein Zugriff auf den Router - FESTE IP DAUERHAFT, PORT 44158 IMMER OFFEN

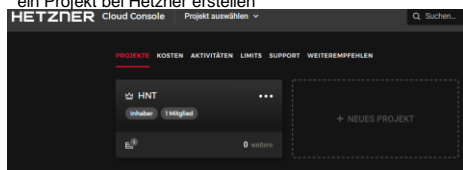


Lösung mit dem Mango MiniRouter für eine feste IP und das PortForwarding (DSL/KABEL/LTE)
Vorbereitung

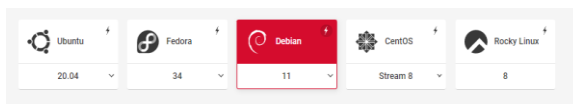
- [account auf diversen VPS Anbietern, in unserem Beispiel von https://accounts.hetzner.com/login](https://accounts.hetzner.com/login)
- ein Consolen-Programm, in unserem Beispiel <https://www.putty.org/>
- ein VPN Wireguard fähiges Gerät, in unserem Beispiel der GL-iNet Mango (Amazon = gl inet mango)
(geht auch mit dem RUT240 LTE Router)

Step-by-Step

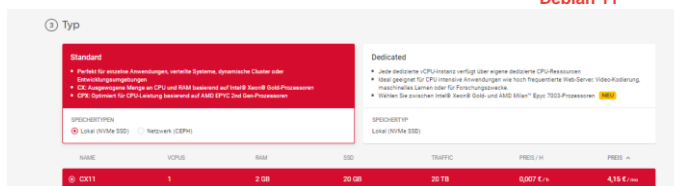
- 1) ein Projekt bei Hetzner erstellen



- 2) einen VPServer hinzufügen



Debian 11

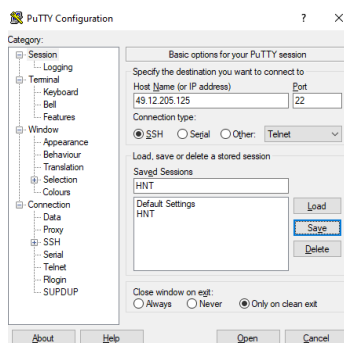


- 3) E-Mails checken für Zugangsdaten vom Server
IHR NEUER SERVER

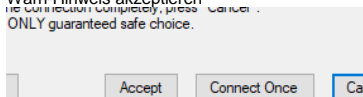
Ihr Server "debian-2gb-nbg1-1" wurde erstellt!
Mit den folgenden Daten können Sie sich an Ihrem Server anmelden:

IPv4	49.	35
IPv6	2a01.	15c/64
Benutzer	root	
Passwort	Px	9Ei4u4M/Wim

- 4) Putty starten

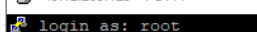


- IP aus der Mail von Hetzner eingeben
- bei Saved Sessions einen namen festlegen und speichern
- Session auswählen und Open drücken
- Warn-Hinweis akzeptieren



- 5) Es öffnet sich die Konsole

49.12.205.125 - PuTTY



- Login als "root" enter
- Passwort aus der Mail kopieren, mit Rechtsklick in die Console wird es eingesetzt (unsichtbar, weil passwort) - dann enter
- Passwort wiederholen wegen NEU vergabe

- d) neues Passwort festlegen - enter
neues Passwort erneut eingeben - enter nicht das man sich vertippt hat
wir sind auf dem VPS angekommen und starten nun die Konfiguration

```
49.12.205.125 - PuTTY
login as: root
root@49.12.205.125's password:
# Pre-authentication banner message from server:
# You are required to change your password immediately (administrator enforced)
#
# End of banner message from server
You are required to change your password immediately (administrator enforced).
Linux debian-2gb-mbgl-1 5.10.0-8-amd64 #1 SMP Debian 5.10.46-4 (2021-08-03) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Sep 4 10:18:03 2021 from 91.64.235.23
Changing password for root.
Current password:
New password:
Retype new password:
root@debian-2gb-mbgl-1:~#
```

- 6) folgende Befehle werden von uns eingegeben:

```
apt update      enter
apt upgrade     enter mit "y" bestätigen enter
apt install iptables enter          ( es kommt nur eine Versions Prüfung, wenn nicht kommt mit "y" bestätigen enter
apt install wireguard enter        mit "y" bestätigen enter
```

- 7) nun müssen wir zwei KEYS erstellen für den späteren VPN

```
cd /etc/wireguard/ enter
wg genkey | tee privatekey | wg pubkey > publickey enter
```

- 8) die Keys lassen wir uns nun mit anderen befehlen anzeigen und speichern sie in einem Text Dokument

```
cat privatekey enter
cat publickey enter
root@debian-2gb-hell-3:/etc/wireguard# wg genkey | tee privatekey | wg pubkey > publickey
root@debian-2gb-hell-3:/etc/wireguard# cat privatekey
6D9xzbY0JTLStfgr0ozQAXeg33iUkB2D57mBQ/rbzHo=
root@debian-2gb-hell-3:/etc/wireguard# cat publickey
Ycvgc9DnffYwT9pN4UTci4sOsrEcEnMiYlFL7XBsWSs=
```

- 9) nun konfigurieren wir den wireguard auf dem server

```
nano /etc/wireguard/wg0.conf enter
es öffnet sich dieses fenster
```

```
49.12.205.125 - PuTTY
GNU nano 2.9.4 /etc/wireguard/wg0.conf
#
# This file can be used to configure wireguard directly. You may wish to create a separate interface (tgw0)
# which only has the wireguard interface as its peer, and enable IP forwarding.
#
# Interface
#
# This section contains the configuration for the wireguard interface.
#
# Interface name
#
# This is the name of the interface. It must be unique and not conflict with any other interface name.
#
# Address
#
# This is the IP address of the interface. It must be a valid IP address.
#
# Netmask
#
# This is the netmask of the interface. It must be a valid netmask.
#
# ListenPort
#
# This is the port that the interface will listen on. It must be a valid port number.
#
# PrivateKey
#
# This is the private key of the interface. It must be a valid private key.
#
# PostUp
#
# This is the command that will be executed after the interface has been created.
#
# PostDown
#
# This is the command that will be executed after the interface has been destroyed.
#
# Peer
#
# This section contains the configuration for the peers that the interface will connect to.
#
# Peer name
#
# This is the name of the peer. It must be unique.
#
# PublicKey
#
# This is the public key of the peer. It must be a valid public key.
#
# AllowedIPs
#
# This is the list of IP addresses that the peer is allowed to connect to.
#
# Endpoint
#
# This is the endpoint that the peer will connect to.
#
# PersistentKeepalive
#
# This is the interval in seconds between keepalive messages.
#
# ExitOnNoPeers
#
# This is a boolean value that determines whether the interface should exit if there are no peers.
#
# SaveConfig
#
# This is a boolean value that determines whether the configuration should be saved.
#
# Help
#
# This is a list of help topics.
#
# Write Out
#
# This is a list of write out topics.
#
# Read File
#
# This is a list of read file topics.
#
# Replace
#
# This is a list of replace topics.
#
# Paste
#
# This is a list of paste topics.
#
# Execute
#
# This is a list of execute topics.
#
# Location
#
# This is a list of location topics.
#
# Justify
#
# This is a list of justify topics.
#
# Go To Line
#
# This is a list of go to line topics.
```

dort kopiert ihr folgenden text rein und ersetzt vorher den private key

[Interface]

ListenPort = 51820

PrivateKey = <setzt hier den Privatekey ein cat privatekey>

Address = 10.0.1.1/24

MTU = 1420

PostUp = iptables -A FORWARD -p tcp --tcp-flags SYN,RST SYN -j TCPMSS --set-mss 1240

PostUp = iptables -A FORWARD -i wg0 -j ACCEPT; iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

PostUp = iptables -A FORWARD -i eth0 -o wg0 -p tcp --syn --dport 44158 -m conntrack --ctstate NEW -j ACCEPT

PostUp = iptables -A FORWARD -i eth0 -o wg0 -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

PostUp = iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 44158 -j DNAT --to-destination 10.0.1.2

PostDown = iptables -D FORWARD -p tcp --tcp-flags SYN,RST SYN -j TCPMSS --set-mss 1240

PostDown = iptables -D FORWARD -i wg0 -j ACCEPT; iptables -t nat -D POSTROUTING -o eth0 -j MASQUERADE

PostDown = iptables -D FORWARD -i eth0 -o wg0 -p tcp --syn --dport 44158 -m conntrack --ctstate NEW -j ACCEPT

PostDown = iptables -D FORWARD -i eth0 -o wg0 -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

PostDown = iptables -t nat -D PREROUTING -i eth0 -p tcp --dport 44158 -j DNAT --to-destination 10.0.1.2

[Peer]

PublicKey = <später setzen wir hier den hotspot-publickey ein>

AllowedIPs = 10.0.1.2/32

Endpoint = 0.0.0.0:51820

drückt Strg+X gefolgt von Y und enter
wir sind zurück in der Konsole

10) nun müssen wir zwei KEYS generieren für unseren VPN Mini Router

a) **wg genkey | tee hotspot-privatekey | wg pubkey > hotspot-publickey** enter
cat hotspot-privatekey enter
cat hotspot-publickey enter

diese speichern wir uns wieder unter der gleichen oder eine anderen txt datei ab

```
root@debian-2gb-hell-3:/etc/wireguard# wg genkey | tee hotspot-privatekey | wg pubkey > hotspot-publickey
root@debian-2gb-hell-3:/etc/wireguard# cat hotspot-privatekey
UElpR/2u/CZiVAJK9JQh9WpfKqKyDck//mz/rMVGHVQ=
root@debian-2gb-hell-3:/etc/wireguard# cat hotspot-publickey
7EvHJZTc34AUBlmX5WhWcAQhTo2gie/fAHtfToIJTyY=
```

b) wir öffnen wieder die konfiguration um den key nachzutragen

nano /etc/wireguard/wg0.conf enter

löscht den text <später setzen> und setzt den public hotspot key ein
drückt strg+x und anschließend y

```
[Peer]
PublicKey = <später setzen wir hier den hotspot-publickey ein>
AllowedIPs = 10.0.1.2/32
Endpoint = 0.0.0.0:51820
```

c) noch eine letzte Konfiguration mit folgenden befehl

echo net.ipv4.ip_forward=1 >> /etc/sysctl.conf enter
sysctl -p enter
systemctl start wg-quick@wg0 enter
systemctl status wg-quick@wg0.service enter

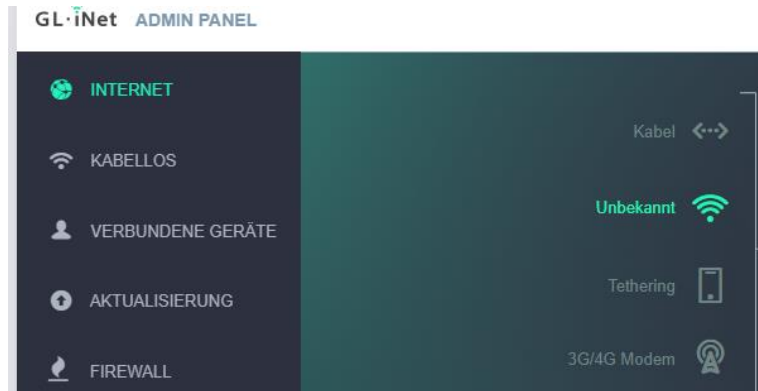
wenn alles Fertig ist sieht es so und eure **Wireguard Server ist active** sieht es so aus , macht mal ne Pause :)

```
root@debian-2gb-hell-3:/etc/wireguard# systemctl status wg-quick@wg0.service
● wg-quick@wg0.service - WireGuard via wg-quick(8) for wg0
   Loaded: loaded (/lib/systemd/system/wg-quick@.service; disabled; vendor preset: enabled)
   Active: active (exited) since Wed 2021-09-08 21:16:13 CEST; 10s ago
     Docs: man:wg-quick(8)
           man:wg(8)
           https://www.wireguard.com/
           https://www.wireguard.com/quickstart/
           https://git.zx2c4.com/wireguard-tools/about/src/man/wg-quick.8
           https://git.zx2c4.com/wireguard-tools/about/src/man/wg.8
   Process: 1891 ExecStart=/usr/bin/wg-quick up wg0 (code=exited, status=0/SUCCESS)
  Main PID: 1891 (code=exited, status=0/SUCCESS)
    CPU: 63ms

Sep 08 21:16:13 debian-2gb-hell-3 wg-quick[1891]: [#] ip link add wg0 type wireguard
Sep 08 21:16:13 debian-2gb-hell-3 wg-quick[1891]: [#] wg setconf wg0 /dev/fd/63
Sep 08 21:16:13 debian-2gb-hell-3 wg-quick[1891]: [#] ip -4 address add 10.0.1.1/24 dev wg0
Sep 08 21:16:13 debian-2gb-hell-3 wg-quick[1891]: [#] ip link set mtu 1420 up dev wg0
Sep 08 21:16:13 debian-2gb-hell-3 wg-quick[1891]: [#] iptables -A FORWARD -p tcp --tcp-flags SYN,RST SYN -j TCPMSS --set-mss 1240
Sep 08 21:16:13 debian-2gb-hell-3 wg-quick[1891]: [#] iptables -A FORWARD -i wg0 -j ACCEPT; iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
Sep 08 21:16:13 debian-2gb-hell-3 wg-quick[1891]: [#] iptables -A FORWARD -i eth0 -o wg0 -p tcp --syn --dport 44158 -m conntrack --ctstate NEW -j ACCEPT
Sep 08 21:16:13 debian-2gb-hell-3 wg-quick[1891]: [#] iptables -A FORWARD -i eth0 -o wg0 -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
Sep 08 21:16:13 debian-2gb-hell-3 wg-quick[1891]: [#] iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 44158 -j DNAT --to-destination 10.0.1.2
Sep 08 21:16:13 debian-2gb-hell-3 systemd[1]: Finished WireGuard via wg-quick(8) for wg0.
root@debian-2gb-hell-3:/etc/wireguard#
```

11) nun geht es zur Konfiguration unseres Mangos Mini Routers

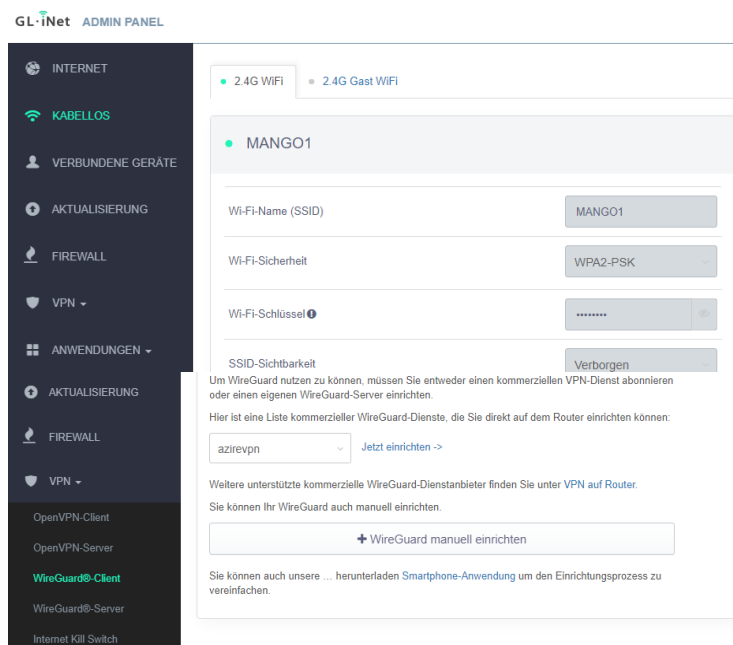
- a) bei Internet suchen wir uns die Quelle aus worüber wir erstmal Internet bekommen. Im Beispiel ist es das WLAN namens Unbekannt



- b) bei Kabellos können wir entweder das vorhandene WLAN so stehen lassen oder legen unser eigenes WLAN fest. Im Beispiel haben wir es Mango1 genannt und ist nicht sichtbar.

- c) bevor wir in der Firewall den Port freigeben können müssen wir Wireguard konfigurieren

- d) wir möchten einen WireGuard Client manuell einrichten



- e) wir nehmen die Daten wie aus dem Bild

der private Key ist der Hotspot-Privatekey

der öffentliche Key ist der publickey vom server (nicht der hotspot key)

Endpunkt ist die IP von Hetzner mit der Erweiterung :51820 bei den erlaubten IPs nehmen wir: 0.0.0.0/0,::/0 nicht wie auf dem Bild.

Anwenden

HNT1	
Schnittstelle	
IP-Adresse	10.0.1.2/32
privater Schlüssel	EBngsyN9gQxbwXg47Rk...
auf Port hören	51820
DNS	
MTU	1420
Peer	
öffentlicher Schlüssel	BQyqg1ry7gFx+Rkh8lrJzJ...
Endpunkt	49.12.205.125:51820
erlaubte IPs	0.0.0.0/0
Aktiv halten	25
PresharedKey	
<div>Entfernen Anwenden</div>	
<div>+ neues Profil erstellen</div>	

10.0.1.2/32

Zugriff auf lokales Netzwerk erlauben.
Und auf Verbinden drücken.

● WireGuard®-Client

⚠ Wenn Sie VPN aktiviert haben, das VPN jedoch keine Verbindung zu seinem Server herstellen kann, gibt es eine Fehlermeldung. Wenn Sie den Server wechseln, während VPN verbunden ist, wird VPN nicht durchgelassen.

Status Management

Zugriff auf lokales Netzwerk erlauben 

Server HNT1

Verbinden


Copyright © 2021 GL.iNet. Alle Rechte vorbehalten.

wenn alles geklappt hat sieht es
wie auf dem Bild aus.
Wenn der Punkt vorne grün ist,
ist die VPN Verbindung aktiv.

● WireGuard®-Client

⚠ Wenn Sie VPN aktiviert haben, das VPN jedoch keine Verbindung zu seinem Server herstellen kann, gibt es eine Fehlermeldung. Wenn Sie den Server wechseln, während VPN verbunden ist, wird VPN nicht durchgelassen.

Status Management

Zugriff auf lokales Netzwerk erlauben 

Server HNT1

IP-Adresse 10.0.1.2
Upload / Download 180 B / 92 B

Trennen

Jetzt gehen wir auf Firewall und
erstellen noch die Portweiterleitung

● Firewall

Port Weiterleitung Öffnen Sie die Ports am Router DMZ

Mit Port Weiterleitungen können entfernte Computer eine Verbindung zu einem bestimmten Computer in der Firewall im lokalen LAN herstellen (z.B. Web-Server, FTP-Server, usw.)

Liste der Regeln

+ Fügen Sie eine neue Konfiguration hinzu

Jetzt legen wir die IP für
unseren Miner noch fest

INTERNET
KABELLOS
VERBUNDENE ...
AKTUALISIERUNG
FIREWALL
VPN
ANWENDUNGEN...
MEHR EINSTELLUNGEN...

Admin Passwort
LAN IP-ADRESSE
Zeitzone
MAC-Adresse klonen
IPv6
Benutzerdefinierter DNS-Server
Tasteneinstellungen
Netzwerk-Architektur
Firmware zurücksetzen

LAN IP Gast IP

● LAN IP-ADRESSE

GL-Router nutzen 192.168.8.1 als standard LAN-IP-Adresse. Dies ist die Adresse, die Sie in die Adressleiste Ihres Browsers eingeben würden, um auf die Admin-Seite des Routers zuzugreifen. Sie können eine innerhalb dieser drei Bereiche manuell einrichten: 192.168.x.x, 172.16.16-31.x.x oder 10.x.x.x

⚠ Hinweis: Die Start-IP-Adresse und die End-IP-Adresse müssen im Bereich von 2 bis 254 liegen, und die End-Adresse sollte größer als die Start-Adresse sein.

LAN IP-ADRESSE 192.168.8.1

Start-IP-Adresse 192.168.8.100

End-IP-Adresse 192.168.8.249

● Statische IP-Adressbindung

Normalerweise wird die IP-Adresse Ihres Computers vom Router dynamisch zugewiesen. Wenn Ihr Computer eine statische IP-Adresse haben soll, können Sie die MAC-Adresse Ihres Computers und die statische IP-Adresse, die Sie verwenden möchten, manuell hinzufügen.

⚠ Beachten Sie, dass der konfigurierte Client sich neu verbinden muss, um aktiv zu werden.

Liste der statischen IP-Bindung 0

+ Fügen Sie eine neue Konfiguration hinzu

die interne IP ist dann die IP vom Miner.

Externe Zone ist wireguard


anwenden

Fügen Sie eine neue Port-Weiterleitungs-Regel hinzu

Name	HNTPort
Interne IP	192.168.8.136
Externe Zone	wireguard
Externe Ports	44158
Interne Ports	44158
Interne Zone	lan
Protokoll	Abbrechen Anwenden TCP
Status	Enabled

sollte dann so aussehen wenn es fertig ist

Port-Prüfung <https://www.yougetsignal.com/tools/open-ports/>



Port Forwarding Tester

your external address

65.108.52.107

open port finder

Remote Address Port Number

[Use Current IP](#)

Check a port's status by entering an address and port number above.

about

The open port checker is a tool you can use to check your external IP address and detect open ports on your connection. This tool is useful for finding out if your port forwarding is setup correctly or if your server applications are being blocked by a firewall. This tool may also be used as a port scanner to scan your network for ports that are commonly forwarded. It is important to note that some ports, such as port 25, are often blocked at the ISP level in an attempt to prevent malicious activity.

For more a comprehensive list of TCP and UDP ports, check out [this Wikipedia article](#).

If you are looking for a software solution to help you configure port forwarding on your network, try using this powerful [Port Forwarding Wizard](#).

If my tool has been helpful to you, check out my [desktop wallpaper](#) site or follow me on Twitter [@kirkouimet](#). Also, if your router is causing you massive grief try picking up a cheap Netgear N600 on [Amazon](#).

common ports

- 21 FTP
- 22 SSH
- 23 TELNET
- 25 SMTP
- 53 DNS
- 80 HTTP
- 110 POP3
- 115 SFTP
- 135 RPC
- 139 NetBIOS
- 143 IMAP
- 194 IRC
- 443 SSL
- 445 SMB
- 1433 MSSQL
- 3306 MySQL
- 3389 Remote Desktop
- 5632 PCAnywhere
- 5900 VNC
- 25565 Minecraft
- Scan All Common Ports

©2009 [Kirk Ouimet Design](#). All rights reserved. [Privacy Policy](#). Hosted by [VPSServer.com](#).