Raspberry Pi mit WireGuard als VPN Server

31. März 2019 von mb-press

Aufbau und Setup

- Raspberry Pi 3 mit Raspbian Stretch Lite
- der Pi hängt im LAN hinter dem Hauptrouter
- LAN: 192.168.150.0/24 (Pi: 192.168.150.200)
- VPN Netz: 10.10.10.0/24 (VPN Server: 10.10.10.1, VPN Client1: 10.10.10.2, VPN Client2: 10.10.10.3)
- Clients als Road Warrior (Android Smartphone und Windows 10 Notebook)

Installation

WireGuard auf dem Raspberry Pi installieren. (Zur Vereinfachung alles als root.)

Raspbian Stretch

```
$ apt-get update
```

```
$ apt-get upgrade
$ apt-get install raspberrypi-kernel-headers
$ echo "deb http://deb.debian.org/debian/ unstable main" | tee --append
$ apt-get install dirmngr
$ apt-key adv --keyserver keyserver.ubuntu.com --recv-keys 8B48AD624692
$ printf 'Package: *\nPin: release a=unstable\nPin-Priority: 150\n' | t
$ apt-get update
$ apt-get install wireguard
$ reboot
```

Raspbian Buster (07.07.2019)

```
$ apt-get update
$ apt-get upgrade
$ apt-get install raspberrypi-kernel-headers
$ echo "deb http://deb.debian.org/debian/ unstable main" | tee --append
$ apt-key adv --keyserver keyserver.ubuntu.com --recv-keys 04EE7237B7D4
$ printf 'Package: *\nPin: release a=unstable\nPin-Priority: 150\n' | t
$ apt-get update
$ apt-get install wireguard
$ reboot
```

Aktivieren von IPv4 forwarding in der **/etc/sysctl.conf**

```
# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward = 1
```

Den Pi neu starten und die Änderungen nochmal überprüfen.

```
$ sysctl net.ipv4.ip_forward
net.ipv4.ip_forward = 1
```

Keys generieren

Die Erstellung der keys wird im Verzeichnis **/etc/wireguard** durchgeführ
Um sicherzustellen dass alle Dateien die richtigen Berechtigungen habe
muss die umask auf 077 gesetzt sein.

```
$ umask 077
```

Server Key generieren

private und public key für den Server

```
$ wg genkey | tee server-private.key | wg pubkey > server-public.key

$ ls -l server*
-rw------- 1 root root 45 Mar 31 10:38 server-private.key
-rw------- 1 root root 45 Mar 31 10:38 server-public.key
```

Client Keys generieren

private und public key für die Clients

```
$ wg genkey | tee client1-private.key | wg pubkey > client1-public.key
$ wg genkey | tee client2-private.key | wg pubkey > client2-public.key

$ ls -l client*
-rw------- 1 root root 45 Mar 31 10:41 client1-private.key
-rw------- 1 root root 45 Mar 31 10:41 client1-public.key
-rw------- 1 root root 45 Mar 31 10:41 client2-private.key
-rw------- 1 root root 45 Mar 31 10:41 client2-public.key
```

Server Konfiguration

Dazu wird die Datei **/etc/wireguard/wg0.conf** erstellt. (Die neue VPN Schnittstelle ist **wg0**.)
Bei den iptables Regeln muss ggf. noch der Name der Netzwerkschnittstelle angepasst werden! Bei mir ist es **eth0**.

```
[Interface]
Address = 10.10.10.1/24
ListenPort = 51820
```

```
PrivateKey = <server-private.key einfügen>
PostUp = iptables -A FORWARD -i %i -j ACCEPT; iptables -A FORWARD -o %i
PostDown = iptables -D FORWARD -i %i -j ACCEPT; iptables -D FORWARD -o

# Client1 Smartphone
[Peer]
PublicKey = <client1-public.key einfügen>
AllowedIPs = 10.10.10.2/32

# Client2 Notebook
[Peer]
PublicKey = <client2-public.key einfügen>
AllowedIPs = 10.10.10.3/32
```

Client Konfiguration

Für jeden Client erstelle ich eine eigene Konfigurationsdatei.

/etc/wireguard/client1.conf

```
[Interface]
PrivateKey = <client1-private.key einfügen>
Address = 10.10.10.2
DNS = 192.168.150.20

[Peer]
PublicKey = <server-public.key einfügen>
Endpoint = vpn.your-public-server.net:51820
AllowedIPs = 0.0.0.0/0, 192.168.150.0/24
PersistentKeepalive = 25
```

/etc/wireguard/client2.conf

```
[Interface]
PrivateKey = <client2-private.key einfügen>
Address = 10.10.10.3
DNS = 192.168.150.20
```

```
[Peer]
PublicKey = <server-public.key einfügen>
Endpoint = vpn.your-public-server.net:51820
AllowedIPs = 0.0.0.0/0, 192.168.150.0/24
PersistentKeepalive = 25
```

Als **DNS** Server nutze ich meinen eigenen im lokalen LAN und mit **0.0.0.0/0** wird alles (der komplette traffic) durch das VPN geroutet.
Da ich mich hinter einem NAT befinde, wird mit **PersistentKeepalive = 25** versucht die Verbindung aufrecht zu halten.

WireGuard starten

```
$ wg-quick up wg0
[#] ip link add wg0 type wireguard
[#] wg setconf wg0 /dev/fd/63
[#] ip address add 10.10.10.1 dev wg0
[#] ip link set mtu 1420 up dev wg0
[#] iptables -A FORWARD -i wg0 -j ACCEPT; iptables -A FORWARD -o wg0 -j
```

WireGuard beim Systemstart automatisch laden.

```
$ systemctl enable wg-quick@wg0
Created symlink /etc/systemd/system/multi-user.target.wants/wg-quick@wg
```

WireGuard Status

Status der aktiven wg0 Schnittstelle.

```
$ wg
interface: wg0
  public key: 9EHJpPuO59RsFbejPZacyZ34TkT7Exas/ZKQsAfTU0U=
  private key: (hidden)
  listening port: 51820

peer: mSOXtoZPSCoZL48u9IZGlpov5T4jAwZ7yhETTDosHVU=
  allowed ips: 10.10.10.2/32
```

```
peer: 9q9PAKC5MUNaF4QmcH5hoqwpWoX2R4/KewvLi0SebmQ=
  allowed ips: 10.10.10.3/32
```

Firewall Konfiguration

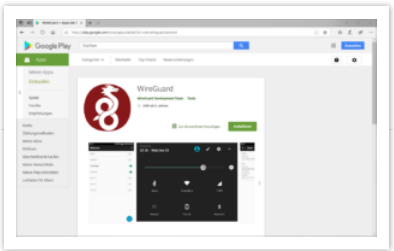
Der **UDP Port 51820** muss an den internen VPN Server weitergeleitet werden. (hier für meinen MikroTik Router)

```
/ip firewall filter
add action=accept chain=forward dst-port=51820 protocol=udp

/ip firewall nat
add action=dst-nat chain=dstnat dst-port=51820 in-interface=wan protoco
```

Road Warrior – Android Client

Für Android nehme ich die offizielle WireGuard App aus dem Google Play Store.



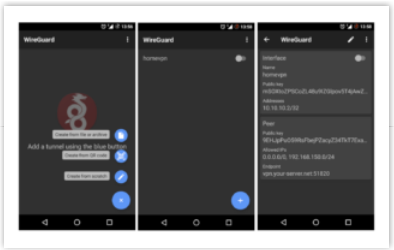
Die Einstellungen der App kann mittels einer Datei, QR-Code oder manuell erfolgen. Auf dem Server wird ein QR-Code für den Client1 erstellt.

```
$ apt install -y qrencode
```

QR-Code für den Client1 erstellen.

```
$ qrencode -t ansiutf8 < client1.conf
```

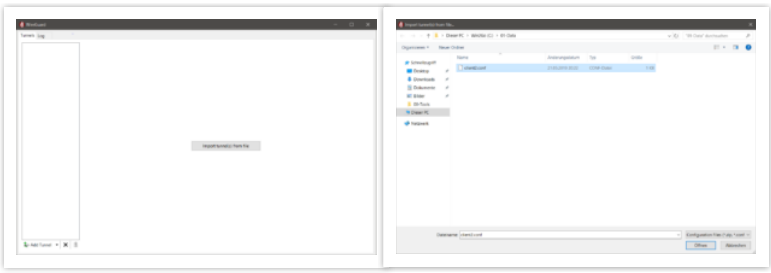
Abscannen und fertig. Ohne die mühselige tipperei auf dem Smartphone.



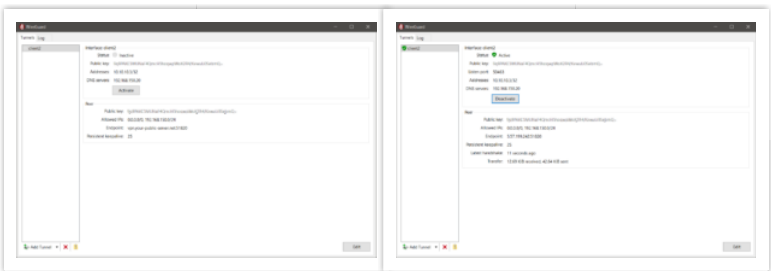
Road Warrior – Windows Client

Für Windows nehme ich den offiziellen WireGuard Client.

Nach der Installation die (auf dem Server erzeugte) **client2.conf** importieren



und die VPN Verbindung aktivieren.



Road Warrior – Linux Client

… kommt …

Fazit

Im Vergleich zu OpenVPN ist die Einrichtung und Konfiguration, trotz der langen Anleitung, in wenigen Minuten erledigt.
Der Tunnelaufbau und das Routing funktionierten auf Anhieb reibungslos und schnell.

17.05.2019 – Nach ca. 6 Wochen bin ich immer noch mehr als zufrieden! Schneller Tunnelaufbau und immer eine stabile Verbindung!

Links

- https://www.wireguard.com
- https://github.com/adrianmihalko/raspberrypiwireguard
- https://emanuelduss.ch/2018/09/wireguard-vpn-road-warrior-setup

Raspberry Pi
‹ UniFi Video NVR Konfiguration automatisch sichern
› PC schaltet sich bei der BitLocker Passworteingabe einfach aus

63 Gedanken zu “Raspberry Pi mit WireGuard als VPN Server”

Sven
8. Mai 2019 um 14:40 | Antworten

unter Debian BUSTER musste ich noch im ersten Schritt die PGP Keys installieren:

```
apt-key adv --keyserver keyserver.ubuntu.com --recv-keys
04EE7237B7D453EC
apt-key adv --keyserver keyserver.ubuntu.com --recv-keys
7638D0442B90D010
```

mb-press
8. Mai 2019 um 22:06 | Antworten

Danke für die Info.

SFTB
2. Juni 2019 um 13:47 | Antworten

Eine Erweiterung um IPv6 wäre nett. Ich habe leider einen DS-Lite Anschluss und somit nur eine IPv6 Adresse

mb-press
6. Juni 2019 um 20:52 | Antworten

Da kann ich momentan leider nichts zu schreiben.
– Habe keinen IPv6 Anschluss.
– Bisher keine Erfahrung mit IPv6.

Jones
26. Juni 2019 um 10:13 | Antworten

Danke für die Anleitung. Kann ich mit dieser Konfiguration auch auf die Geräte im Heimnetz (bei Dir 192.168.150.0/24) zugreifen. Ich habe einen Medienserver und möchte über die Wireguard-Anbindung im Urlaub darauf zugreifen können. Zudem möchte ich auch ssh Zugriff auf den Pi haben.

Danke

mb-press
28. Juni 2019 um 20:21 | Antworten

Wenn der VPN Tunnel verbunden ist, kannst du auf alle Geräte im LAN zugreifen.

Gustav
26. Juni 2019 um 17:39 | Antworten

Hallo,
mit dem Artikel konnte ich wunderbar schnell folgendes erreichen (Danke!):
* Smartphone (iOS) baut erfolgreich Tunnel auf: Handshake wird in App und wg angezeigt. OK
* Über DNS-Angabe in client.conf werden mir die DNS-Anfragen des Clients auch in Pi-hole angezeigt. OK
* Es gibt im Client aber keinen Seitenaufbau. Ich gehe davon aus, dass der Traffic (sprich Request an gewünschten Server) den WireGuard-Server nach erfolgreichem DNS gar nicht verlässt, also weder mit der VPN-IP (weil: im MikroTik-Router in ARP-Liste kein Eintrag) aber offensichtlich auch nicht auf die IP des Servers

umgesetzt von der NAT-Maquerade-Regel.

Haben Sie andere Ideen, wo es haken könnte am „Tunnelausgang“? Iptables? Etwas anderes?

Danke und viele Grüße

mb-press
28. Juni 2019 um 20:27 | Antworten

Da würde ich spontan auf die Firewall tippen. Einfach mal zum testen kurz deaktivieren.
Hast du auch im MikroTik Router die beiden Firewall Regeln gesetzt?

Gustav
29. Juni 2019 um 02:02 | Antworten

Danke für Deine Antwort: Ja. Beide liefern auch hochzählende Paketzahlen.
Aber: wenn ich die beiden Regeln richtig verstehe sind sie für den INBOUND des VPN-Tunnels zuständig. Der Handshake kommte ja zu Stande; dort hatte ich daher keine Fehlerquelle mehr gesehen.

Wenn ich in meinem DNS-Resolver (pi-hole) die passenden Requests mit der IP aus dem Tunnel sehe, scheint der DNS-Teil am „Tunnelende“ ja auch zu gehen (wireguard + pi-hole laufen auf dem selben Server).

Mir scheint daher plausibel: Entweder kommt die DNS-Antwort nicht zum VPN-Client oder in der Folge der (zur IP aufgelöste) Request des VPN-Clients kommt nicht aus dem Requesttunnel per NAT. Im MikroTik müsste doch dann Traffic mit der LAN-IP meines Servers zu sehen sein, weil der NAT am Tunnelende den Traffic der Clients auf sich NATted, richtig? Wenn dem so wäre, dann müsste doch die „PostUp“-Anweisung an iptables nicht greifen. Sehen kann ich Sie zumindest in iptables nach start von wireguard.

Dummerweise weiß ich darüber hinaus überhaupt nicht, wie man so etwas prüft/analysiert. Ich habe noch nie an irgend einem Sever mit iptables etwas zu tun gehabt, weil ich immer schon Fritzbox + MikroTik im Einsatz habe…

Gustav
29. Juni 2019 um 02:57 | Antworten

Nun habe ich doch selber die Ursache gefunden:
Analyse iptables mit `sudo iptables -t nat -L -nv` zeigt: Keine Pakete.
in ifconfig noch mal nachgeschaut: Finde dort kein **eth0** (mehr), aber heute **em1** (zumindest bei ubuntu server). Wenn man in wg0.conf die iptables-Anweisung entsprechend anpasst, geht es auch! Blöde Falle, viel Zeit zum EInkreisen der Ursache gebraucht und am Ende ist es immer ganz einfach gewesen – wenn man es vorher gewusst hätte.

Vielelicht wäre oben im Text ein Hinweis sinnvoll, dass die Wired-Schnittstelle bei manchen Systemen statt eth0 em1 heißt und das ggf. angepast werden muss. Vielleicht spart es einem anderen die Forschungsarbeit… :)

Noch mal: Danke Dir für Deine wirklich hilfereiche Anleitung!

mb-press
29. Juni 2019 um 11:38

Hab das bei der Server Konfiguration noch ergänzt. Danke für den Hinweis.

Henrik
28. Juni 2019 um 20:14 | Antworten

Hi mb-press,
ich habe auf meinem Raspberry PI das Wireguard nach deiner Anleitung installiert und es läuft auch soweit. Nur wenn ich nun versuche von meinem Iphone über die App eine Verbindung zu meinem Tunnel aufzubauen kommt immer die Meldung im Log
„Handshake did not complete after 5 seconds“
„Sending Handshake initiation“
Und das immer wieder.
Zudem hab ich in den VPN Option von IOS beim Server immer die IP 127.0.0.1 also Localhost. Hast du ne Idee woran das liegen

könnte das die Verbindung nicht aufgebaut wird.

Zudem wundert mich noch in der Serverconfig warum du oben bei der IP des Servers nen /24 Netz hast und unten bei den Clients ein /32 Netz?

Würde mich über ein Feedback von dir freuen.

Grüße Henrik

mb-press
28. Juni 2019 um 22:32 | Antworten

Hallo Henrik,

den „Handshake did not complete after 5 seconds“ Fehler hatte ich (zum Glück) noch nicht.
Mein Windows 10 Notebook und Android Smartphone funktionieren bisher mit dem Setup problemlos.

was du mal versuchen könntest:
– andere Geräte funktionieren?
– aktuelle WireGuard IOS App?
– localhost beim Server ist sehr merkwürdig, kannst du das ändern?
– entferne mal in der client.conf den DNS Eintrag
– ändere mal in der client.conf die allowed ips von 0.0.0.0/0 auf

Der VPN Server hängt in einem /24 Netz.
Da der Client dem Server kein komplettes Netzwerk zur Verfügung stellt, sondern nur einen Host, ist bei einem Road Warrior Setup die Netzmaske /32.

Gruß, Michael …

Gustav
29. Juni 2019 um 02:16 | Antworten

Hallo Henrik,
das hatte ich auch mal kurz. Ursache war bei mir, dass der QR-Code augenscheinlich alles ins iphone lieferte, aber der Public-Key leider nicht der richtige war. Schau Dir mal oben den Screenshot mit den beiden Public-Keys an und vergleiche mit den beiden wg.conf und client1.conf… so muss es aussehen. War bei mir aber nicht. Nachdem ich den Public-Key des Clients anpasste (entweder im iphone oder in conf), ging der handshake auf Anhieb. :)

Mir war auch etwas rätselhaft, wie der pubic-Key des Clients in den QR-Code kommen sollte, wenn er gar nicht in der conf für die *qrencode* enthalten ist. Ich habe vermutet, dass das iphone sich dann selber einen generiert aus dem Private-Key. Wohlmöglich ist der QR-Code korrekt, wenn man in der client1.conf auch noch zusätzlich den Public-Key des Clients unter [Interace] einfügt. Hab’s noch nicht versucht (Wegen meines anderen Problems siehe oben), aber wäre denkbar.

Gustav
29. Juni 2019 um 03:41 | Antworten

Ergänzung nach Test:

* Es geht nicht, den erzeugten public-key des client in client1.conf zusätzlilch zu legen.
* Mit dem selben Private-Key des clients erzeugt zumindest bei mir *wg pubkey* einen anderen Key als der iOS-Client beim einlesen des QR-Codes. Das ist bei Dir vermutlich auch die Ursache. Unglücklich irgendwie…bis diese technisch Abweichung gelöst ist, muss man wohl manuell den Code vom iphone auf den Server bringen und in der wg0.conf eintragen.

Die Frage ist: Das müssten ja alle iOS-User haben und was kann man daran ändern. Gibt es eine Paramter zu *wg pubkey*, um die selbe Ableitung wie der iOS-Client zu bekommen?

Gustav
30. Juni 2019 um 13:02 | Antworten

Ergänzung:
Es scheint so, dass der generierte public key nur manchmal abweicht zwischen *wg pubkey* und iOS. Ich hatte jetzt wieder einige Fälle ohne Abweichungen, aber einzelne mit. Wenn man den manuellen workaround nicht mag, kann man also einfach eine neue private/public key-Kombi erzeugen und schauen, ob es passt.

Thema habe ich wireguard bereits gemeldet mit reproduzierbarem Beispiel; man darf nicht vergessen, es ist halt noch immer beta-Phase… :)

Jones
1. Juli 2019 um 20:38 | Antworten

Hallo,

Danke für die Anleitung. Installation auf dem Pi3 neuste Raspbian (Buster) funktionierte wunderbar. Die Verbindung wird aufgebaut. Nur leider habe ich keinen Zugriff auf das Internet bzw. aud die lokale Resourcen.

Heimnetz (FritzBox 6490 10.0.0.1) 10.0.0.0/24 Netz
Pi3 10.0.0.60
Der Rest ist wie bei Dir. Also Wireguard-Server 10.0.1.1, Client1 10.0.1.2, Client2 10.0.1.3. Portweiterleitung in der FritzBox usw.

root@raspberrypi:/etc/wireguard# wg
interface: wg0
public key: gQ5/FY3ReWV+ZTZP+v8R….
private key: (hidden)
listening port: 51822

peer: QYR2wdtKD6rGZPcsS4lJzGLiHv+…….
endpoint: 46.114.xx.xxx:55702
allowed ips: 10.0.1.2/32
transfer: 9.11 KiB received, 5.66 KiB sent

peer: 1PBMEIQRqIxOLEtlHr2b27valj5/8a…..
allowed ips: 10.0.1.3/32

Da ich nicht der größte Netzwerkexperte bin, hoffe ich auf Hilfe.
Welche Informationen kann ich senden um
1. Internet zu nutzen
2. auf das Netzt 10.0.0.0/24 zuzugreifen.

Danke Jones

mb-press
2. Juli 2019 um 00:36 | Antworten

Hallo Jones,

von was für einem Client aus geht es denn nicht? (Gerät / Betriebssystem)

Überprüfe mal die Server Config.
– dein WireGuard Port ist 51822, richtig?
– stimmt der Name der Netzwerkschnittstelle bei den iptables Regeln? (den Fehler hatten wir nämlich schon mal)

Jones
2. Juli 2019 um 09:19 | Antworten

Habs gelöst. Die FritzBox Kindersicherung war für den Pi aktiviert. Habe es hiermit gemerkt:

root@raspberrypi:/etc/wireguard# curl ip.stigok.com
302 Document moved302 Document movedThis document has moved here.
root@raspberrypi:/etc/wireguard#

Nach der Freischaltung klappte dann auch der Handshake.

Danke noch einmal für die Anleitung. Vielleicht baust du den „Onlinetest“ ja in deine Beschreibung ein. Sozusagen als Vorbedingung für alle weiteren Schritte.

Danke

mb-press
2. Juli 2019 um 22:58 | Antworten

Da muss man erst mal drauf kommen. ;)
Freut mich das es läuft!

Jones
4. Juli 2019 um 10:43 | Antworten

Habe noch eine abschließende Bemerkung/Hilfegesuch. Mit der Geschwindigkeit scheint in einigen Situationen etwas nicht zu stimmen. Ich habe eine 100/50 (FB 6490) Anbindung. Diese wird auch voll geliefert. Zuhause an der FritzBox hängt der Pi3B+ per Gbit an der FB. Ein lokaler Speedtest auf dem Pi (speedtest-cli) lieferte die volle Geschwindigkeit (100/50). Auf der Wireguard Gegenseite (Netzwerkanbindung 500/500) steht mein Reiserouter GL.Inet 750S-Ext. Der Wireguard Client ist hier bereits vom Hersteller impementiert.

Nun mein Problem: Steht die Wireguard Verbindung und führe ich mit dem Client ein Speedtest durch (auch mit Kabel verbunden), liefert der Speedtest die Werte (ca. 40/45). Soweit so gut. Wenn ich jetzt aber eine Plex Video Stream (23Mbit/s) starte, dann ist die Verbindung offenbar auf 15-20 Mbit/s begrenzt (sehe ich im FritzBox Onlinemonitor). Alle 5-10 Sekunden gibt es daher Aussetzer im Video. Ein 23 Mbit/s Plex Stream ohne Wireguard Verbindung läuft einwandfrei. Auch höhere Streamraten (bis 40 Mbit) habe ich bereits geschafft.

Wie kommt es, dass ein Speedtest 45 Mbit/s schafft, ein Plex Stream aber nicht einmal die Hälfte. Die Prozessoren beider Geräte (Pi und Gl.Inet) sind bei weitem nicht ausgelastet. An der Vernetzung der Geräte kann wie gesagt nicht liegen. Habt ihr ein paar Ansatzpunkte?

Thomas
6. Juli 2019 um 18:27 | Antworten

@Jones: Der GBit LAN Port des Pi3B+ schafft maximal ca. 300 Mbit/s Durchsatz = ca. 37,5 MB/s.
Die Performance im „echten Leben“ wird bspw. bei Streamen von Videos von einer angeschlossenen USB Festplatte niedriger sein – da alle Daten (USB Ports und LAN) trotzdem durch den SoC und den einen USB 2.0 Port laufen müssen.

Erst der Pi4 bietet vollen GBit Durchsatz (ca. 940Mbit) da dieser voll angebunden ist.

Buntstift
7. Juli 2019 um 19:49 | Antworten

Hallo,
leider klappt es bei mir auf einem 3B+ mit Buster nicht. Die unstable-sourcen werden abgelehnt, weil sie nicht signiert sind und das Paket Wireguard wird nicht gefunden. Was muss ich tun, damit ich es installieren kann?
Danke und Gruß

mb-press
7. Juli 2019 um 21:08 | Antworten

Habs gerade mal ausprobiert. Wie Sven es oben beschrieben hat!
apt-key adv `--keyserver keyserver.ubuntu.com --recv-keys 04EE7237B7D453EC`

Damit hat es bei mir (Pi 3 mit Buster) funktioniert.

Buntstift
7. Juli 2019 um 22:16 | Antworten

Jo, stimmt. Danke für den Hinweis. Hatte ich oben leider überlesen.

Sven_A
8. Juli 2019 um 09:15 | Antworten

Hallo,

vielen Dank für die Anleitung, VPN funktioniert, und auch der Zugriff vom Client auf’s Heimnetz klappt.
Da ich eine Fritzbox habe wollte ich jetzt am Handy einen SIP Client nutzen. Dabei ist mir aufgefallen:

Das Handy ist mit seiner VPN Adresse nicht aus dem Heimnetz erreichbar.
Abhilfe: Auf der Fritzbox eine Statische IPv4 Route setzen die aufs Wireguard Netz verweist.

Um bei den Verwendeten Beispieladressen zu bleiben:
Auf der Fritzbox wird eine Route mit dem
Ziel-Netz: 10.10.10.0/24
Gateway: 192.168.150.200
gesetzt, damit klappt auch SIP Telefonie und der direkte Zugriff aus dem Heimnetz (192.168.150.0/24) aufs VPN Netz (10.10.10.0/24)

Viele Grüße,
Sven

mb-press
8. Juli 2019 um 19:08 | Antworten

Sehr interessant, vielen Dank für die Info!

Blobba
9. Juli 2019 um 15:49 | Antworten

@Sven_A: Danke für den Tip. Nach der Lösung für mein VoIP Problem über WireGuard habe ich schon lange gesucht. Einfach die IPv4 Route in der FB angelegt und schon klappt es auch mit der FritzApp Fon von unterwegs.

Buntstift
10. Juli 2019 um 20:22 | Antworten

Hallo,

ich habe noch ein Problem. Ich habe Wireguard wie hier beschrieben. Es läuft auf einem Pi 3B+ parallel zu Pi-Hole mit Stubby hinter einer Fritzbox. Das läuft so weit alles gut und ich kann mich problemlos per Wireguard verbinden und auch auf alle lokalen Geräte zugreifen. Nur komme ich über Wireguard nicht ins Internet -> Meldung „DNS_PROBE_FINISHED_BAD_CONFIG“. Als DNS ist in der WG-Config der Pi angegeben.

Leider habe ich keinen Ansatz, wo ich anfangen könnte zu suchen. Habt ihr Tipps oder vielleicht sogar eine Lösung für dieses Problem?

mb-press
10. Juli 2019 um 21:43 | Antworten

Fritzbox rebooten und auch mal zum testen einen anderen DNS Server eintragen.

Buntstift
11. Juli 2019 um 09:40 | Antworten

Wenn ich die FritzBox als DNS angebe funktioniert es. Die FritzBox verweist als DNS wieder auf den Pi. Wenn ich den Pi direkt als DNS angebe funktioniert es nicht. Fehlt da evtl. noch eine Route auf dem Pi? Die hier in den Kommentaren genannte Route auf der FritzBox habe ich eingetragen.

Frank
7. August 2019 um 16:28 | Antworten

Hoi habe selbiges Problem. Gibts ne lösung ?

Frank
7. August 2019 um 16:31 | Antworten

ach ja noch eine info .. unter stretch hatte ich das problem nicht , sondern nur unter buster.

Frank
11. Juli 2019 um 11:10 | Antworten

Einfach mal ein **DICKES DANKE** für die Anleitung.
Läuft prima!
Frank

mb-press
20. Juli 2019 um 12:29 | Antworten

Danke, freut mich! :-)

Juergen
15. Juli 2019 um 18:34 | Antworten

Moin,

ich bekomme beim Aufruf von

```
sudo apt-get install wireguard
Reading package lists... Done
Building dependency tree
Reading state information... Done
E: Unable to locate package wireguard

cat /etc/os-release
PRETTY_NAME="Raspbian GNU/Linux 9 (stretch)"
NAME="Raspbian GNU/Linux"
VERSION_ID="9"
VERSION="9 (stretch)"
ID=raspbian
```

```
ID_LIKE=debian
```

Kann ich bitte einen Tipp bekommen, was ich nun tun sollte?

Juergen
15. Juli 2019 um 19:07 | Antworten

Habs jetzt hinbekommen
Hatte alles mit sudo gemacht und tee schlug dann mangels sudo fehl

i.c.h.
8. August 2019 um 18:08 | Antworten

Guten Abend Juergen,
Genau vor diesem Problem stehe ich auch, wie hast Du das Problem denn gelöst?
Ich möchte eigentlich vermeiden den Root User einzurichten.

Vielen Dank im Voraus

i.c.h.
8. August 2019 um 18:16 | Antworten

> Nevermind. Als Neuling habe ich was missverstanden jetzt geht es auch bei mir.

mopz
22. Juli 2019 um 09:03 | Antworten

egal was ich probiere ich bekomm immer die Meldung:
gpg: Empfangen vom Schlüsselserver fehlgeschlagen: Server indicated a failure
bei allen 3 keys hier auf der seite der selbe fehler…

mb-press
23. Juli 2019 um 20:06 | Antworten

> Trag mal den DNS Server von Google (8.8.8.8) in die /etc/resolv.conf ein und probiers dann noch mal.

mopz
23. Juli 2019 um 22:38 | Antworten

@mb-press

Super!!!
Vielen dank das wars!!

Ist ja komisch es stand mein DSL router als dns drin…

Robin
8. August 2019 um 18:16 | Antworten

Hallo,

beim Starten von WireGuard über „$ wg-quick up wg0“ erhalte ich in der dritten Zeile diese Fehlermeldung:

Key is not in the correct lenght or format :
Configuration parsing error

Kennt jemand von euch diese Meldung und kann mir weiterhelfen?

Danke

mb-press
8. August 2019 um 20:14 | Antworten

Dann stimmt was mit dem Format des eingefügten keys nicht! ;)

Hast du vielleicht den Pfad zu der Datei dort eingetragen? Hier muss nur der Inhalt der entsprechenden *.key Datei rein.

Uwe
10. August 2019 um 18:27 | Antworten

@mb-press

Endlich mal eine Anleitung ohne viel Schnick-Schnack, die auf Anhieb funktioniert.
Super!
Vielen Dank!

mb-press
11. August 2019 um 11:18 | Antworten

Danke! :-)

Walter
17. August 2019 um 22:48 | Antworten

Super Anleitung. Hat alles auf Anhieb ohne Probleme funktioniert!

Eine Frage hätte ich noch: Wenn eine neue Wireguard Version rauskommt, einfach
apt-get update
apt-get upgrade
machen?

mb-press
18. August 2019 um 11:44 | Antworten

Ja, Wireguard kann über die Paketverwaltung aktualisiert werden.

Aber aus eigener Erfahrung:
Backup machen! WireGuard configfiles (/etc/wireguard) und auch mal ein komplettes Image der SD Karte!
Bei einem Wireguard Update hat es mir mal den kompletten Pi zerschossen, da ging nix mehr.

Vorsicht auch bei Kernel Updates des Pi. Danach passen die WireGuard Module natürlich nicht mehr zum neuen Kernel.
Lässt sich meistens mit einer Neuinstallation von Wireguard wieder hinbekommen, aber auch nicht immer. ;)

Walter
19. August 2019 um 15:40 | Antworten

Image der SD-Karte mach ich wie?

mb-press
19. August 2019 um 18:32 | Antworten

Da kann ich diese beiden Programme empfehlen:
Win32 Disk Imager
USB Image Tool

Die SD-Karte in den Windows Rechner und dann mit dem Programm ein Image des Datenträgers erstellen.

Stephan
12. September 2019 um 21:18 | Antworten

Hallo,

bin absoluter Neuling.
VPN Verbindung steht, allerdings keine Verbindung auf die Synology im eigenen Netzwerk…
QR- Code klapte also auch.
Fehlermeldung auf IOS: „Handshak did not cpmplete after 5 sec…“

Ich gehe davon aus, dass es am Port liegt:

/ip firewall filter
add action=accept chain=forward dst-port=51820 protocol=udp
/ip firewall nat
add action=dst-nat chain=dstnat dst-port=51820 in-interface=wan protocol=udp to-addresses=192.168.150.200 to-ports=51820

Wo genau trage ich das ein?

Den Rest habe ich fünfmal gecheckt…

Wie gesagt, Neuling :-)

Danke!

mb-press
14. September 2019 um 11:10 | Antworten

Zur IOS Fehlermeldung gibt’s hier schon einige Kommentare.

Die Einträge für die Firewall und das Portforwarding sind vom verwendeten Router abhänging.
In meinem Fall bezieht sich das auf einen MikroTik Router.
Die Regeln weden über das CLI (Terminal) eingegeben.

Was für einen Router hast du denn?

Stephan
14. September 2019 um 12:36 | Antworten

Hallo,

danke für die schnelle Antwort.
Ich habe einen Telekom Hybrid Router…. Ich weiß, würde auch lieber auf FB oder ähnliches umstellen.
Doch leider ist das aufgrund meines Anschlusses nicht möglich, da ich ohne Hybrid wahrscheinlich den langsamsten Anschluss der Welt habe :-(

Firewall ist beim hybrid- Router leider nicht deaktivierbar… Die o.g. Lösungen habe ich alle schon probiert… Leider ohne Erfolg.
Beim Router habe ich den Port 51820 geöffnet.

Wahrscheininlich ist die Frage zu trivial aber ich stelle sie mal trotzdem : Wie und wo gebe ich die Regeln über das CLI ein :-)

Wie gesagt, ist das erste mal das ich etwas „programmiere „:-))

Vielen Dank und schönes WE
Stephan

mb-press
14. September 2019 um 14:10 | Antworten

Auf keinen Fall die Firewall deaktivieren!

Wenn du den Port 51820 offen hast, nimmt der Router die Verbindung von draussen schonmal an.
Jetzt musst du sie nur noch an den Raspi weiterleiten.

Google mal nach „Telekom Hybrid Router Port Weiterleitung“
https://www.telekom.de/hilfe/downloads

/bedienungsanleitung-speedport-hybrid.pdf, Seite 105

Der Router hat kein CLI. Kann nur über die Weboberfläche konfiguriert werden.

Thomas B.
17. September 2019 um 19:46 | Antworten

Ganz großes Lob. Für mich die beste Anleitung zu Wireguard die ich nach umfangreicher Recherche gefunden habe.
Dank dieser Anleitung war die Einrichtung von Wireguard auf meinem Raspberry Pi4 ein Klacks, während andere Anleitungen nur ein Fragezeichen hinterließen…
Habe nun Handy und Windows-Notebook über Wireguard angebunden. – Vielen Dank !

mb-press
18. September 2019 um 18:53 | Antworten

Danke für das dicke Lob! :-)

Thomas B.
29. September 2019 um 11:58 | Antworten

Was mich noch interessieren würde: Momentan betreibe ich neben dem Wireguard-Raspberry noch eine LAN-2-LAN Kopplung über das Internet mit der VPN-Funktion von zwei Fritzboxen.

Diese VPN Verbindung ist wegen der Fritzbox-CPU-Leistung leider nicht sehr performant. – Hier wäre die Frage, wenn ich auf beide Seiten/in beide lokalen Netze Wireguard-Gateways (=Raspberrys) packe, wie müsste ich die dann für eine LAN-2-LAN-Kopplung einrichten ? – An den Fritzboxen müsste ich dann nur die IP des jeweiligen Wireguard-Raspberrys als Gateway für das jeweils andere Netz als statische Route angeben, denke ich. – Der normale Internetverkehr der beiden Standorte soll ja ganz normal über die Fritzbox direkt ins Internet laufen.

kellerassel
28. September 2019 um 08:08 | Antworten

Moin,
bei mir läuft alles wunderbar.

Nur:
Hat jemand eine Idee, wie man den Android-Client nach der nächtlichen Zwangstrennung des DSL-Anschlusses wieder neu startet,
um die neue IP-Adresse zu bekommen?

mb-press
28. September 2019 um 09:26 | Antworten

Bei dynamischen IPs einfach einen DynDNS Dienst nutzen.

kellerassel
28. September 2019 um 11:41 | Antworten

Ist schon klar, aber einmal aus- und wieder einschalten bleibt, weil WG selbst nicht wieder nachschaut, wenn es aktiviert wurde.

Sebastian
5. Oktober 2019 um 21:35 | Antworten

Könnt ihr etwas zur Performance sagen? Ich habe 100Mbit Upstream und würde gerne wissen, ob der Pi3 dies hier in Wireguard rausholen kann.
Auf meinem DD-WRT Router (Linksys WRT1900ACS v2) ist die Performance unterirdisch, ich kriege maximal 8-10 MBit/sec Transferrate. OpenVPN hingegen läuft auf demselben Router mit ca. 30MBit/sec. Dies ist insbesondere deshalb seltsam, weil alle die Performance von Wireguard loben, aber ich vermute, dass es im DD-WRT nicht vernünftig integriert wurde.

Wie sieht es hier mit der Raspi Performance aus?

Georg
1. November 2019 um 12:57 | Antworten

Hallo,
Eine Frage: gibt es schon eine Möglichkeit, WireGuard auf einem RasberryPi 4 mit neuem Buster zu nutzen? Welche Vorteile hat dies: höherer Durchsatz/ Geschwindigkeit? Hat es schon jemand erfolgreich probiert?

mb-press
3. November 2019 um 13:17 | Antworten

Denke das sollte laufen, habs aber noch nicht ausprobiert.

Schreibe einen Kommentar

Name *

E-Mail *

Website

Mit der Nutzung dieses Formulars erklärst du dich mit der Speicherung und Verarbeitung deiner Daten durch diese Website einverstanden. *

Kommentar abschicken