Eigener VPN-Server mit WireGuard in einem LXD-Container

Oct 21, 2026 · @Sebastian Ebner · Quelle: KI Werkzeug Cloude

Überblick

Am Ende läuft auf einem eigenen Linux-Server ein WireGuard-VPN in einem LXD-Container. Das Handy geht dauerhaft über diesen VPN ins Internet und tritt immer mit der festen IP-Adresse des Servers auf. Das ist nützlich, um die eigenen Aufrufe aus einer Besucherstatistik zu filtern, in fremden WLANs verschlüsselt zu surfen oder Zugänge auf die eigene Adresse zu beschränken.

Der Weg eines Datenpakets: Handy → öffentliche IP des Servers, UDP-Port 51820 → LXD leitet den Port in den Container weiter → WireGuard (`wg0`) entschlüsselt → der Container gibt das Paket mit der Server-Adresse ins Internet weiter.

Voraussetzungen:

- Ein Linux-Server (z. B. Ubuntu) mit root-Zugang und eigener öffentlicher IPv4-Adresse, LXD ist installiert und eingerichtet (`lxd init`).
- Ein Android-Handy mit der WireGuard-App und Termux (für SSH und Dateikopie).
- Platzhalter in dieser Anleitung: `HOST-IP` = öffentliche Adresse des Servers, `CONTAINER` = Name des Containers, `NETZ` = Name des LXD-Netzes, `CONTAINER-IP` = interne Adresse des Containers.

Alle Befehle werden als root ausgeführt. Welche auf dem Host und welche im Container laufen, steht jeweils dabei. Die Eingabezeile im Terminal (`root@…`) zeigt, wo man gerade ist.

1. Vorab prüfen (auf dem Host)

```
modprobe wireguard && lsmod | grep wireguard
curl -4 -s ifconfig.me; echo
lxc network list
ufw status
```

- **Erste Zeile:** Erscheint `wireguard` , kann der Kernel WireGuard. LXD-Container nutzen den Kernel des Hosts.
- **Zweite Zeile:** zeigt die öffentliche IP = `HOST-IP` .

- **Dritte Zeile:** zeigt den Namen des LXD-Netzes = `NETZ`. Er heißt oft `lxdbr0`, kann aber anders lauten. Er wird für die Firewall gebraucht.
- **Vierte Zeile:** ob eine Firewall aktiv ist.

Läuft der Server selbst schon als Container beim Anbieter, prüft `ip link add wgtest type wireguard && echo OK && ip link del wgtest`, ob WireGuard dort direkt geht. Dann lässt sich alles auch ohne eigenen LXD-Container einrichten (Schritte 3 bis 5 direkt auf dem Server).

2. Container und Portweiterleitung (auf dem Host)

Container anlegen, WireGuard-Modul und Autostart setzen:

```
lxc init ubuntu:24.04 CONTAINER -c linux.kernel_modules=wireguard -c
boot.autostart=true
lxc start CONTAINER
lxc list CONTAINER
```

In der Spalte IPv4 steht die interne Adresse, z. B. `10.x.x.x (eth0)`. Das ist `CONTAINER-IP`. Später steht dort zusätzlich die WireGuard-Adresse `10.8.0.1 (wg0)`. Gemeint ist immer die eth0-Adresse.

Adresse fest einstellen und den UDP-Port weiterleiten:

```
lxc config device override CONTAINER eth0 ipv4.address=CONTAINER-IP
lxc config device add CONTAINER wgport proxy listen=udp:HOST-IP:51820
connect=udp:CONTAINER-IP:51820 nat=true
lxc config device show CONTAINER
```

In der Ausgabe muss ein Eintrag `wgport` mit `nat: "true"` stehen. LXD legt die Weiterleitung selbst an, auf dem Host lauscht dabei kein Programm auf Port 51820. Das ist richtig so.

Firewall (nur wenn `ufw status` „active“ zeigt):

```
ufw allow 51820/udp
ufw allow in on NETZ
ufw route allow in on NETZ
ufw route allow out on NETZ
```

Zusätzlich muss eine Firewall im Kundenmenü des Anbieters, falls vorhanden, UDP 51820 durchlassen.

3. WireGuard einrichten (im Container)

In den Container wechseln mit `lxc exec CONTAINER -- bash`. Die Eingabezeile zeigt dann den Containernamen.

Installieren und Schlüssel erzeugen:

```
apt update && apt install -y wireguard iptables
mkdir -p /etc/wireguard && cd /etc/wireguard && umask 077
wg genkey | tee server.key | wg pubkey > server.pub
wg genkey | tee handy.key | wg pubkey > handy.pub
echo 'net.ipv4.ip_forward=1' > /etc/sysctl.d/99-wg.conf && sysctl -w
net.ipv4.ip_forward=1
```

Server-Konfiguration anlegen und starten (Block komplett einfügen):

```
cd /etc/wireguard
cat > wg0.conf <<EOF
[Interface]
Address = 10.8.0.1/24
ListenPort = 51820
PrivateKey = $(cat server.key)
PostUp = iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
PostDown = iptables -t nat -D POSTROUTING -o eth0 -j MASQUERADE

[Peer]
PublicKey = $(cat handy.pub)
AllowedIPs = 10.8.0.2/32
EOF
systemctl enable --now wg-quick@wg0
wg show
```

`wg show` muss `interface: wg0` und einen `peer` zeigen. Fehlt das, zeigt `systemctl status wg-quick@wg0 --no-pager` den Grund.

4. Handy-Konfiguration erzeugen und übertragen

Im Container (`HOST-IP` durch die echte Adresse ersetzen):

```
cd /etc/wireguard
cat > /root/handy.conf <<EOF
[Interface]
PrivateKey = $(cat handy.key)
Address = 10.8.0.2/32
DNS = 9.9.9.9

[Peer]
PublicKey = $(cat server.pub)
Endpoint = HOST-IP:51820
AllowedIPs = 0.0.0.0/0, ::/0
PersistentKeepalive = 25
EOF
exit
```

`AllowedIPs = 0.0.0.0/0, ::/0` schickt den gesamten Verkehr durch den VPN, auch IPv6. Sonst ginge das Handy über IPv6 am VPN vorbei.

Auf dem Host die Datei aus dem Container holen und abmelden:

```
lxc file pull CONTAINER/root/handy.conf /root/handy.conf
exit
```

In Termux auf dem Handy (Eingabezeile `~ $`, nicht `root@…`):

```
termux-setup-storage
scp root@HOST-IP:/root/handy.conf ~/storage/downloads/
```

`termux-setup-storage` fragt einmal nach der Speicherberechtigung. Diesen Befehl einzeln eingeben und die Frage beantworten, erst dann `scp`. Sonst wird die nächste Zeile als Antwort verschluckt.

Der QR-Code-Weg (`qrencode`) eignet sich nur, wenn der Code auf einem anderen Gerät angezeigt wird. Die WireGuard-App scannt nur mit der Kamera, nicht aus einem Screenshot.

5. Android einrichten und testen

1. WireGuard-App öffnen → „+“ → „Aus Datei oder Archiv importieren“ → `handy.conf` aus „Downloads“ wählen → einschalten. Android fragt einmal nach der VPN-Erlaubnis.
2. Android-Einstellungen → Netzwerk → VPN → Zahnrad bei WireGuard → **„Durchgehend aktives VPN“** einschalten. Optional **„Verbindungen ohne VPN blockieren“**: Dann geht nichts mehr am VPN vorbei, auch nicht kurz nach dem Neustart.

3. **Test am Handy:** `https://ifconfig.me` im Browser öffnen. Angezeigt werden muss `HOST-IP`.
4. **Test auf dem Host:** `lxc exec CONTAINER -- wg show`. Unter `peer` muss „latest handshake“ mit einer Zeitangabe stehen.
5. **Aufräumen:** `handy.conf` aus „Downloads“ löschen, auf dem Host `rm /root/handy.conf` und im Container `lxc exec CONTAINER -- rm /root/handy.conf /etc/wireguard/handy.key`. Der private Handy-Schlüssel soll nur noch in der App liegen.

Einzelne Apps ausnehmen: In der WireGuard-App den Tunnel bearbeiten → „Alle Anwendungen“ → „Ausschließen“. Ausgenommene Apps haben aber kein Internet mehr, solange „Verbindungen ohne VPN blockieren“ aktiv ist.

6. Fehlerbehebung

Meldung oder Beobachtung	Ursache	Lösung
`Error: No value found in "10.x.x.x 10.8.0.1"` beim Portweiterleiten	Container-Adresse automatisch ausgelesen, dabei kam die wg0-Adresse mit	`CONTAINER-IP` von Hand eintragen, nur die eth0-Adresse
`scp: /root/handy.conf: No such file or directory`	`scp` auf dem Server statt in Termux ausgeführt, oder Datei liegt noch im Container	Mit `exit` abmelden bis `~ $`; vorher `lxc file pull` auf dem Host
`termux-setup-storage: command not found`	Befehl auf dem Server eingegeben	Erst abmelden, dann in Termux
`wg show` zeigt nichts	Konfiguration nicht gespeichert oder Dienst nicht gestartet	`ls /etc/wireguard`, dann `systemctl enable --now wg-quick@wg0`
Kein „latest handshake“	Port nicht durchgereicht oder Firewall blockt	`lxc config device show CONTAINER` prüfen; ufw-Regeln mit dem echten Netznamen; Anbieter-Firewall UDP 51820
VPN verbunden, aber keine Webseiten	Weiterleitung oder NAT fehlt	`sysctl net.ipv4.ip_forward` muss 1 sein; `PostUp`-Zeile mit `-o eth0` prüfen

Meldung oder Beobachtung	Ursache	Lösung
Nach Neustart kein VPN	Modul oder Autostart fehlt	`lxc config set CONTAINER linux.kernel_modules wireguard` und `boot.autostart true`
Bei Paste in Termux fehlen Leerzeichen (`systemctlenable`)	Zeilenumbruch beim Einfügen	Befehl einzeln neu eingeben

7. Hinweise

- **Sicherheit:** Der WireGuard-Port antwortet nur auf Pakete mit gültigem Schlüssel und ist für Portscanner praktisch unsichtbar. Die eigentliche Angriffsfläche des Servers bleibt SSH. Prüfen mit `ss -tulpn`: Von außen sollte nur Port 22 offen sein.
- **Container ohne Root-Rechte:** `lxc config get CONTAINER security.privileged` sollte leer sein, `lxc config get core.https_address` ebenfalls (LXD nicht übers Netz steuerbar).
- **Handy verloren:** Im Container den `[Peer]`-Block aus `/etc/wireguard/wg0.conf` löschen und `systemctl restart wg-quick@wg0`. Danach kommt dieses Handy nicht mehr in den VPN.
- **Weiteres Gerät:** eigenes Schlüsselpaar erzeugen, einen zweiten `[Peer]`-Block mit `AllowedIPs = 10.8.0.3/32` anhängen, in dessen Konfiguration `Address = 10.8.0.3/32`.
- **Gemeinsame IP mit anderen Diensten:** Läuft auf demselben Server ein Tor-Dienst (z. B. EOTK), kommen Onion-Besucher mit derselben Adresse an wie das eigene Handy. Eine Besucherzählung darf diese Adresse dann nur für Nicht-Onion-Zugriffe ausnehmen.
- **Updates:** im Container und auf dem Host `unattended-upgrades` installieren, damit Sicherheitsupdates automatisch kommen.