

KNOWLEDGE BASE · PUBLIC DOCUMENT

WireGuard on a VPS: your own VPN, step by step

VPS & Servers

CODE

RLX-INT-KB-5076

VERSION

v2026.10.15

COUNTRY · LANGUAGE

International · English

MozOut International

RLX Holdings (Pty) Ltd. · Group RLX Holdings

Tax no. (SARS) 943 907 6234 · Registration no. (CIPC) 2025/667953/07

<https://www.my.mozout.com/knowledgebase/5076>



The short answer: WireGuard is a simple, fast VPN you can set up on a Linux VPS in a few minutes. It connects your computer or phone to the server through an encrypted tunnel: to reach what only the server can see, or to send all your browsing through it. You need a VPS with **root access**. It does not work on shared hosting.

WireGuard is open-source third-party software that the customer installs and runs. Our support does not install or repair it: see **How far our support goes**. Before you run a VPN service, read the **Terms and conditions**: what passes through the server is your responsibility.

On the server (Ubuntu 22.04 LTS or similar)

1

Log in over SSH and install. `sudo apt update` and then `sudo apt install wireguard`. If you do not have a sudo user yet, see **how to create one**.

2

Create the server keys:

```
wg genkey | sudo tee /etc/wireguard/server_private.key | wg  
pubkey | sudo tee /etc/wireguard/server_public.key  
sudo chmod 600 /etc/wireguard/server_private.key
```

3

Create the file `/etc/wireguard/wg0.conf` with the content below, replacing the private key with what is in `server_private.key` and leaving the client part for the next step:

```
[Interface]
```

```
Address = 10.8.0.1/24
```

```
ListenPort = 51820
```

```
PrivateKey = (the server private key)
```

```
[Peer]
```

```
PublicKey = (the client public key)
```

```
AllowedIPs = 10.8.0.2/32
```

4

Open UDP port 51820 with `sudo ufw allow 51820/udp`. If ufw is not set up yet, follow **Setting up the ufw firewall without locking yourself out**. If there is another firewall in front of the server, open the port there too.

5

Start it and check: `sudo systemctl enable --now wg-quick@wg0` and then `sudo wg show`. The command should list the interface and the client.

On the phone or computer

1

Install the official WireGuard app. It exists for Windows, macOS, Linux, Android and iOS.

2

Create an empty tunnel. The app generates the client key pair and the private key stays on the device. Copy the client **public key** into the `PublicKey` line on the server and restart with `sudo systemctl restart wg-quick@wg0`.

3

Write the client configuration:

```
[Interface]
```

```
PrivateKey = (generated by the app)
```

```
Address = 10.8.0.2/24
```

```
[Peer]
```

```
PublicKey = (the server public key)
```

```
Endpoint = (your VPS IP):51820
```

```
AllowedIPs = 10.8.0.0/24
```

```
PersistentKeepalive = 25
```

4

Switch the tunnel on and test with `ping 10.8.0.1`. If it answers, the tunnel is up.

Only the VPN network, or all your browsing?

Mode	What it does	What changes
Only the VPN network	The client reaches the server (and what it sees) through the tunnel; the rest of the browsing leaves through the normal connection.	AllowedIPs = 10.8.0.0/24 on the client. Nothing else.
All browsing through the server	Everything the client does leaves with the VPS IP.	AllowedIPs = 0.0.0.0/0 on the client, and forwarding plus NAT on the server (below). The example covers IPv4 only.

For the second mode, switch on forwarding on the server: `sudo sysctl -w net.ipv4.ip_forward=1`, and to keep it after a reboot write `net.ipv4.ip_forward=1` into a file inside `/etc/sysctl.d/`. Then add to the server's `[Interface]` section:

```
PostUp = iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
PostDown = iptables -t nat -D POSTROUTING -o eth0 -j MASQUERADE
```

The name `eth0` is the server's network card: confirm yours with `ip route show default` (it appears after "dev"). With ufw on, you also have to let forwarded traffic through, for example with `sudo ufw route allow in on wg0 out on eth0`.

The private key never leaves the place where it was created. Do not paste it in a chat, an e-mail or a support ticket. Between the client and the server you exchange only the **public** keys.

Each device gets its own `[Peer]` block and its own address (10.8.0.3, 10.8.0.4 and so on). To remove a device, delete its block and restart. More on ports and firewalls in **Ports and firewall on a VPS**.

Built the tunnel and it does not answer? Open a ticket with the output of `sudo wg show` (without the private keys).

[Open a support ticket](#)

SEE ALSO

[Setting up the ufw firewall on Ubuntu without locking yourself out](#)

[Ports and firewall on a VPS: why your app is not reachable](#)

[Keeping your VPS or dedicated server secure: the six that matter](#)

[How far our support goes](#)



Online version of this document

MozOut is a leading internet services company, with a mission to help businesses to be born and prosper through technology.

2020

FOUNDED

37,000+

CLIENTS

130+

SIGN-UPS A DAY

MozOut International

RLX Holdings (Pty) Ltd. • Group RLX Holdings

TAX NO. (SARS)

943 907 6234

REGISTRATION NO.
(CIPC)

2025/667953/07

REGISTERED OFFICE

1111 Olive Street
Saint Louis 63101, Missouri, United States

CONTACT

info@mozout.com • +27 78 823 3325 • www.mozout.com

OPENING HOURS

Monday to Friday - 08 AM to 04 PM
Saturday & Sunday - Closed

RLX-INT-KB-5076 • v2026.10.15 • Generated on 17/10/2026 09:16