

BASE DE CONHECIMENTO · DOCUMENTO PÚBLICO

WireGuard num VPS: a sua própria VPN, passo a passo

VPS e Servidores

CÓDIGO

RLX-MZ-KB-5076

VERSÃO

v2026.10.15

PAÍS · IDIOMA

Moçambique · Português

MozOut Moçambique

RLX Holdings, S.A. · Grupo RLX Holdings

NUIT 401 191 607 · NUEL 105 045 974 · CAE 62022

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



A resposta curta: o WireGuard é uma VPN simples e rápida que se instala num VPS Linux em poucos minutos. Liga o seu computador ou telemóvel ao servidor por um túnel cifrado: para chegar ao que só o servidor vê, ou para enviar toda a sua navegação por lá. Precisa de um VPS com **acesso root**. Não funciona em hospedagem partilhada.

O WireGuard é um programa de código aberto de terceiros, que o cliente instala e gere. O nosso suporte não o instala nem o repara: veja **Até onde vai o nosso suporte**. Antes de montar um serviço de VPN, leia os **Termos e condições**: o que passa pelo servidor é da sua responsabilidade.

No servidor (Ubuntu 22.04 LTS ou semelhante)

1

Entre por SSH e instale. `sudo apt update` e depois `sudo apt install wireguard`. Se ainda não tem um utilizador com sudo, veja **como criar um**.

2

Crie as chaves do servidor:

```
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

Crie o ficheiro `/etc/wireguard/wg0.conf` com este conteúdo, trocando a chave privada pelo que está em `server_private.key` e deixando a parte do cliente para o passo seguinte:

```
[Interface]
```

```
Address = 10.8.0.1/24
```

```
ListenPort = 51820
```

```
PrivateKey = (a chave privada do servidor)
```

```
[Peer]
```

```
PublicKey = (a chave pública do cliente)
```

```
AllowedIPs = 10.8.0.2/32
```

4

Abra a porta UDP 51820 com `sudo ufw allow 51820/udp`. Se o ufw ainda não está montado, siga **Montar o firewall ufw sem se trancar de fora**. Se tiver outro firewall à frente do servidor, abra a porta também lá.

5

Arranque e confira: `sudo systemctl enable --now wg-quick@wg0` e depois `sudo wg show`. O comando deve listar a interface e o cliente.

No telemóvel ou no computador

1

Instale a app oficial do WireGuard. Existe para Windows, macOS, Linux, Android e iOS.

2

Crie um túnel vazio. A app gera o par de chaves do cliente e a chave privada fica no aparelho. Copie a **chave pública** do cliente para a linha `PublicKey` do servidor e reinicie com `sudo systemctl restart wg-quick@wg0`.

3

Escreva a configuração do cliente:

```
[Interface]
PrivateKey = (gerada pela app)
Address = 10.8.0.2/24

[Peer]
PublicKey = (a chave pública do servidor)
Endpoint = (o IP do seu VPS):51820
AllowedIPs = 10.8.0.0/24
PersistentKeepalive = 25
```

4

Ative o túnel e teste com `ping 10.8.0.1`. Se responder, o túnel está de pé.

Só a rede da VPN, ou toda a navegação?

Modo	O que faz	O que muda
Só a rede da VPN	O cliente chega ao servidor (e ao que ele vê) pelo túnel; o resto da navegação sai pela ligação normal.	AllowedIPs = 10.8.0.0/24 no cliente. Nada mais.
Toda a navegação pelo servidor	Tudo o que o cliente faz sai com o IP do VPS.	AllowedIPs = 0.0.0.0/0 no cliente, e no servidor reencaminhamento e NAT (abaixo). O exemplo cobre só IPv4.

Para o segundo modo, ligue o reencaminhamento no servidor: `sudo sysctl -w net.ipv4.ip_forward=1`, e para ficar depois de reiniciar escreva `net.ipv4.ip_forward=1` num ficheiro dentro de `/etc/sysctl.d/`. Depois acrescente à secção `[Interface]` do servidor:

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

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

O nome `eth0` é o da placa de rede do servidor: confirme o seu com `ip route show default` (aparece depois de «dev»). Com o ufw ligado, é preciso ainda deixar passar o tráfego reencaminhado, por exemplo com `sudo ufw route allow in on wg0 out on eth0`.

A chave privada nunca sai do sítio onde nasceu. Não a cole numa conversa, num e-mail nem num pedido de suporte. Entre o cliente e o servidor trocam-se apenas as chaves **públicas**.

Cada aparelho tem o seu próprio bloco `[Peer]` e o seu próprio endereço (10.8.0.3, 10.8.0.4 e assim por diante). Para tirar um aparelho basta apagar o bloco dele e reiniciar. Mais sobre portas e firewall em **Portas e firewall num VPS**.

Montou o túnel e não responde? Abra um pedido com o resultado de `sudo wg show` (sem as chaves privadas).

[Abrir pedido de suporte](#)

VEJA TAMBÉM

Montar o firewall ufw sem se trancar de fora

Portas e firewall num VPS: porque a sua aplicação não responde

Manter o VPS ou servidor dedicado seguro: as seis coisas que contam

Até onde vai o nosso suporte



Versão online deste documento

A MozOut é uma empresa líder em serviços de internet, com a missão de ajudar negócios a nascerem e prosperarem por meio da tecnologia.

2020

FUNDADA

37 mil+

CLIENTES

130+

INSCRIÇÕES POR DIA

MozOut Moçambique

RLX Holdings, S.A. • Grupo RLX Holdings

NUIT 401 191 607

NUEL 105 045 974

CAE 62022

SEDE Bairro 7 de Setembro
Vilankulo 1304 • CEP 0411-02, Inhambane, Moçambique

CONTACTOS info@mozout.com • +258 84 635 1111 • +258 86 635 1111 •
www.mozout.com

HORÁRIO 2ª. à 6ª. Feira - 08 à 16 Horas
Sábado & Domingo - Fechado