

## Langkah Langkah pengerjaan WireGuard

### ✓ 1. Siapkan Interface WireGuard di MikroTik (Winbox GUI)

1. Buka Winbox → Menu: **WireGuard**
  2. Klik tombol + → Tambahkan interface baru:
    - Name: wg0
    - Listen Port: 51820 (default, bisa diganti jika bentrok)
  3. Klik **Apply** dan **OK**
- 

### ✓ 2. Tambahkan WireGuard Peer (Ubuntu VM)

1. Masih di Winbox → Masuk tab **Peers**
  2. Klik +
    - Interface: wg0
    - Public Key: *(isi nanti setelah kita generate dari Ubuntu)*
    - Allowed Address: 192.168.200.2/32 *(alamat IP yang akan digunakan oleh Ubuntu)*
  3. Jangan Apply dulu sebelum kamu punya Public Key dari Ubuntu
- 

### ✓ 3. Setup WireGuard di Ubuntu (CLI)

Install WireGuard:

```
bash
```

Salin kode

```
sudo apt update
```

```
sudo apt install wireguard -y
```

```
sudo apt install resolvconf -y
```

Generate key pair:

```
bash
```

Salin kode

```
wg genkey | tee privatekey | wg pubkey > publickey
```

Lihat hasilnya:

```
cat privatekey
```

cat publickey

Catat keduanya.

---

#### ✅ 4. Tambahkan Public Key Ubuntu ke MikroTik

- Copy hasil cat publickey dari Ubuntu
  - Masukkan ke kolom **Public Key** di peer MikroTik
  - Klik **Apply** dan **OK**
- 

#### ✅ 5. Tambahkan Peer di Ubuntu (wg0.conf)

Buat file config:

Salin kod

```
sudo nano /etc/wireguard/wg0.conf
```

Isi:

[Interface]

PrivateKey = <PRIVATE\_KEY\_UBUNTU>

Address = 192.168.200.2/24

DNS = 1.1.1.1

[Peer]

PublicKey = <PUBLIC\_KEY\_MIKROTIK>

Endpoint = <PUBLIC\_IP\_MIKROTIK>:51820

AllowedIPs = 0.0.0.0/0

PersistentKeepalive = 25

Ganti:

- <PRIVATE\_KEY\_UBUNTU> = hasil dari cat privatekey
  - <PUBLIC\_KEY\_MIKROTIK> = lihat di Winbox → Interface → Public Key
  - <PUBLIC\_IP\_MIKROTIK> = IP publik MikroTik cloud kamu
- 

#### ✅ 6. Aktifkan WireGuard Ubuntu

Salin kode

```
sudo wg-quick up wg0
```

Cek koneksi:

Salin kode

```
ping 192.168.200.1
```

(192.168.200.1 adalah IP MikroTik, kita tambahkan berikutnya)

---

## ✅ 7. Tambah IP dan NAT di MikroTik

1. Masuk Winbox → IP → Addresses → Klik +
  - Address: 192.168.200.1/24
  - Interface: wg0
2. IP → Firewall → NAT → Klik +
  - Chain: dstnat
  - Protocol: tcp
  - Dst. Port: 80
  - Action: dst-nat
  - To Address: 192.168.200.2
  - To Port: 80

(Untuk mengakses web server dari internet)

---

## ✅ Cara Melihat Public Key WireGuard di Winbox:

1. **Buka tab WireGuard di sidebar kiri** (seperti yang sudah kamu lakukan).
2. **Klik tab Interfaces** (yang menampilkan wg0).
3. **Klik dua kali interface wg0** untuk membuka detailnya.
4. Akan muncul jendela baru → **Public Key** akan muncul otomatis di sana, biasanya di bagian bawah dari interface wg0.

Contohnya:

markdown

Salin kode


Private Key: \*\*\*\*\*

Public Key: v8uN5y9skfQm8HktsqLhP0... (← inilah yang kamu copy)

## Langkah 8: Port Forwarding (NAT Rule)

 **Tujuan:** Agar request ke IP publik:8000 diteruskan ke 192.168.200.2:8000

1. Buka **Winbox**
2. Klik menu **IP > Firewall > Tab NAT**
3. Klik tombol **+** (Add)
4. Pada tab **General**:
  - **Chain:** dstnat
  - **Protocol:** tcp
  - **Dst. Port:** 8000
  - **In. Interface:** ether1 (atau interface dengan IP publik)
5. Pindah ke tab **Action**:
  - **Action:** dst-nat
  - **To Addresses:** 192.168.200.2 (ip vpn ubuntu)
  - **To Ports:** 8000 (port yang diatur di backend)
6. Klik **OK**

 Sekarang MikroTik akan meneruskan koneksi dari IP publik port 8000 ke IP Ubuntu via VPN.

---

## Langkah 4: Firewall Filter (Izinkan Forwarding)

 **Tujuan:** Izinkan MikroTik untuk meneruskan traffic TCP port 8000 ke Ubuntu

1. Buka tab **Filter Rules** di dalam **IP > Firewall**
2. Klik tombol **+**
3. Pada tab **General**:
  - **Chain:** forward
  - **Protocol:** tcp
  - **Dst. Port:** 8000
  - **Dst. Address:** 192.168.200.2
4. Pada tab **Action**:
  - **Action:** accept
5. Klik **OK**

Langkah Langkah pengaturan VPN L2TP

### ✅ 1. Atur IP Address di Interface Lokal

Kita kasih IP statis ke MikroTik untuk jaringan VPN (bukan pakai DHCP). Langkah ini dilakukan lewat menu:

**IP > Addresses**

atau via CLI:

bash

Salin kode

/ip address

add address=192.168.100.1/24 interface=ether1 comment="IP lokal VPN"

📌 Catatan:

- IP 192.168.100.1/24 adalah IP MikroTik di jaringan VPN.
  - Kamu bebas ganti jadi subnet lain (asal tidak bentrok).
  - Gunakan interface yang akan dipakai untuk lalu lintas VPN (misal ether1 atau interface bridge).
- 

### ✅ 2. Buat IP Pool untuk VPN Client

Client VPN nanti akan diberi IP dari pool ini. Atur dari:

**IP > Pool**

atau CLI:

bash

Salin kode

- Ip
- Pool
- add name=pool-vpn
- address 192.168.100.10-192.168.100.20
- next pool –

### ✅ Langkah 3: Buat PPP Profile

1. Masuk ke menu **PPP** di Winbox.
2. Pilih tab **Profiles**.
3. Klik tanda “+” untuk buat profile baru.
4. Isi seperti berikut:

Field	Nilai
Name	vpn-profile
Local Address	192.168.100.1
Remote Address	pool-vpn
DNS Server	8.8.8.8 (atau sesuai kebutuhan)
Use Encryption	required (jika ada opsi ini)

✓ Klik **OK**.

---

#### ✓ Langkah 4: Aktifkan L2TP Server

1. Masih di menu **PPP**, klik tab **L2TP Server**.
2. Centang/aktifkan **Enabled**.
3. Pilih **Default Profile**: vpn-profile (yang barusan kamu buat).
4. Centang **Use IPsec** jika ingin pakai IPsec (aman), dan isi Secret (misalnya vpnku123).

✓ Klik **Apply** dan **OK**.

---

#### ✓ Langkah 5: Tambahkan User VPN

1. Masih di menu **PPP**, buka tab **Secrets**.
2. Klik “+” untuk tambah user.
3. Isi:

Field	Nilai
Name	vpnuser
Password	vpnpassword
Service	l2tp
Profile	vpn-profile

#### Langkah 6 NAT Masquerade untuk IP VPN

Kita perlu kasih NAT (masquerade) ke IP pool VPN supaya lalu lintas client VPN bisa diteruskan ke internet.

**Langkah:**

Masuk ke terminal MikroTik atau pakai WinBox:

bash

Salin kode

```
/ip firewall nat add chain=srcnat src-address=192.168.100.0/24 out-interface=ether1 action=masquerade
```

src-address sesuaikan dengan IP pool VPN kamu (misal 192.168.100.0/24). ether1 = interface yang mengarah ke internet (bisa juga pppoe-out1, lihat routing kamu).