AFRIDYNE SYSTEMS · TECHNICAL GUIDE

WireGuard: Connect Two Networks

A fast, simple VPN tunnel between two sites, with configs you can copy.

Updated November 2026 | Debian & Ubuntu gateways | about 20 minutes

A WireGuard tunnel joins two networks, for example an office and a home, so devices on each side can reach the other as if they were on one network. It is fast, small and much simpler to set up than older VPNs. This guide connects two sites; the same method works for a single laptop.

> **Before you start:** you need a Linux machine at each site that can act as the gateway (a small server, mini PC or Raspberry Pi), and at least one site with a reachable public IP address and a router that lets you open one UDP port. Many South African fibre and LTE connections sit behind carrier-grade NAT with no public address. Check with your ISP before you begin.

1. Plan the addresses

Each site needs its own network range, and the tunnel needs a third. **The two sites must not use the same range.** Many routers default to `192.168.0.x` or `192.168.1.x`, which clashes if both sites use it. Change one first.

Item	Site A (has public IP)	Site B
LAN range	`192.168.10.0/24`	`192.168.20.0/24`
Tunnel address	`10.8.0.1`	`10.8.0.2`
Reachable at	`office.example.co.za:51820`	no inbound access needed

2. Install and create keys

On **both** gateways:

both gateways

```
sudo apt install wireguard
wg genkey | sudo tee /etc/wireguard/private.key | wg pubkey | sudo tee /etc/wireguard/public.key
sudo chmod 600 /etc/wireguard/private.key
sudo cat /etc/wireguard/public.key
```

Each machine now has a private key (never share it) and a public key (swap these with the other site). Show the private key with `sudo cat /etc/wireguard/private.key` when you need to paste it into the config below.

3. Configure Site A

Site A: /etc/wireguard/wg0.conf

```
[Interface]
Address = 10.8.0.1/24
ListenPort = 51820
PrivateKey = SITE-A-PRIVATE-KEY

[Peer]
PublicKey = SITE-B-PUBLIC-KEY
AllowedIPs = 10.8.0.2/32, 192.168.20.0/24
```

4. Configure Site B

Site B dials out to Site A, so it needs the endpoint. The keepalive keeps the tunnel open through home routers.

Site B: /etc/wireguard/wg0.conf

```
[Interface]
Address = 10.8.0.2/24
PrivateKey = SITE-B-PRIVATE-KEY

[Peer]
PublicKey = SITE-A-PUBLIC-KEY
Endpoint = office.example.co.za:51820
AllowedIPs = 10.8.0.1/32, 192.168.10.0/24
PersistentKeepalive = 25
```

`AllowedIPs` is the list of addresses that go through the tunnel to that peer: the other gateway and the other site's LAN.

5. Allow routing and open the port

Each gateway must pass traffic between its LAN and the tunnel. On **both**:

both gateways

```
echo "net.ipv4.ip_forward=1" | sudo tee /etc/sysctl.d/99-wireguard.conf
sudo sysctl --system
```

On Site A, also open the port in the firewall, and open the same UDP port on the router, forwarding it to the gateway's LAN address:

Site A

```
sudo ufw allow 51820/udp
```

If you use UFW on the gateways, also allow forwarding between the tunnel and the LAN, replacing `eth0` with the gateway's LAN interface name (`ip a` shows it):

both gateways

```
sudo ufw route allow in on wg0 out on eth0
sudo ufw route allow in on eth0 out on wg0
```

6. Start and test

both gateways

```
sudo systemctl enable --now wg-quick@wg0
sudo wg show
```

A working tunnel shows a recent `latest handshake` under the peer. Then test from each gateway:

Site B

```
ping 10.8.0.1
ping 192.168.10.1
```

Other devices on the LAN: a PC at Site B only knows how to reach `192.168.10.x` if its traffic is sent to the gateway. The easiest fix is a static route on the Site B router: destination `192.168.10.0/24`, next hop the gateway's LAN address. Do the same on Site A for `192.168.20.0/24`.

If it does not connect

- **No handshake at all:** the UDP port is not reaching Site A. Check the router port forward, the firewall, and that the public IP is real (not carrier-grade NAT).
- **Handshake works but pings fail:** check `ip_forward`, the firewall forwarding rules and the static routes.
- **Keys:** each config holds its *own* private key and the *other* site's public key. Swapping them is the most common mistake.