

Secure Remote Access with WireGuard and a VPS Relay

Goal

Connect a remote Windows 11 system to a local office LAN (192.168.1.0/24) that has a Windows 10 + Samba server, using an external VPS (`nyx.omnitech.net`) as a secure hub.

Topology

```
Win11 Client ↔ VPS (nyx.omnitech.net) ↔ Office Linux Server ↔  
192.168.1.0/24 LAN
```

- **VPN Subnet:** 10.10.10.0/24
- **VPS Hub:** 10.10.10.1
- **Office Gateway:** 10.10.10.2
- **Win11 Client:** 10.10.10.3

Step 1: Generate Keys

On **Linux systems** (VPS + Office):

```
sudo mkdir -p /etc/wireguard/keys  
cd /etc/wireguard/keys  
wg genkey | tee private.key | wg pubkey > public.key  
chmod 600 private.key
```

On **Windows 11**:

Use WireGuard client's "Generate Keypair" function.

⚙️ Step 2: VPS Config (/etc/wireguard/wg0-TP.conf)

```
[Interface]
Address = 10.10.10.1/24
ListenPort = 51820
PrivateKey = /etc/wireguard/keys/private.key

# Office
[Peer]
PublicKey = OFFICE_PUB
AllowedIPs = 10.10.10.2/32, 192.168.1.0/24

# Win11
[Peer]
PublicKey = WIN11_PUB
AllowedIPs = 10.10.10.3/32
```

⚙️ Step 3: Office Config (/etc/wireguard/wg0-TP.conf)

```
[Interface]
Address = 10.10.10.2/24
PrivateKey = /etc/wireguard/keys/private.key

[Peer]
PublicKey = VPS_PUB
Endpoint = nyx.omnitech.net:51820
AllowedIPs = 10.10.10.0/24
PersistentKeepalive = 25
```

Enable forwarding + NAT:

```
echo "net.ipv4.ip_forward=1" | sudo tee -a /etc/sysctl.conf
sudo sysctl -p
sudo iptables -t nat -A POSTROUTING -s 10.10.10.0/24 -o eth0 -j MASQUERADE
```

Step 4: Windows 11 Client Config

```
[Interface]
PrivateKey = WIN11_PRIV
Address = 10.10.10.3/24

[Peer]
PublicKey = VPS_PUB
Endpoint = nyx.omnitech.net:51820
AllowedIPs = 192.168.1.0/24, 10.10.10.0/24
PersistentKeepalive = 25
```

Step 5: Testing

On Win11:

```
ping 192.168.1.10    # Windows 10 host
ping 192.168.1.20    # Samba server
```

Access file shares:

```
\\192.168.1.10\share
```

RDP:

```
mstsc -r 192.168.1.10
```

Security Notes

- Linux: private keys stored in `/etc/wireguard/keys/` (chmod 600).
- Configs reference filenames, so secrets aren't embedded in configs.
- Windows: private key must be inline (stored securely by the client).

- SMB is never exposed to the internet — only reachable via VPN.
-