Why a VPN is the Right Solution for Remote SMB Access

🎯 The Challenge

- Remote Windows 11 laptop needs to access a **Windows 10 & Samba server** on an office LAN (`192.168.1.0/24`).
- A public VPS (`nyx.omnitec.net`) is available to bridge connections.
- Exposing SMB (port 445/TCP) directly to the Internet is **dangerous**.
- KISS Rules - what is the simplest solution?
- This VPN is called "TP" - KCS [Keep Configs Separate].

🗺️ Topology

```
Win11 Client  ⟷  VPS (nyx.omnitec.net)  ⟷  Office 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

🔒 Why VPN?

- **Protects SMB traffic** — encrypted tunnel instead of raw TCP/445.
- **Authenticates peers** — only configured clients with keypairs can join.
- **LAN-like experience** — browse `\\192.168.1.10\share` as if on-site.
- **Scales well** — add peers easily without exposing the office firewall.

🚫 Alternatives Compared

Option	Pros	Cons / Risks	Fit
WireGuard (hub)	Secure, fast, easy config	Requires small office gateway config	⭐ Best overall
OpenVPN	Mature, GUI-rich	Heavier, slower	Acceptable alt
Raw SMB forward	Minimal setup	🚫 Exposes 445 to Internet (ransomware)	Do not use
SSH tunnels	Fine for RDP only	Poor for SMB browsing	Limited cases

---

⚙️ WireGuard Advantages

- Modern crypto, small codebase, very fast.
- Simple configs: keys + AllowedIPs.
- Cross-platform (Linux, Windows, macOS, mobile).
- Roaming support (great for laptops).

🛠️ Operations Summary

1. **Generate keys** on VPS & Office server (`/etc/wireguard/keys/` with `600` perms).
2. **Configure** `wg0` on VPS (`10.10.10.1/24`), allow UDP/51820.
3. **Configure** `wg0` on Office (`10.10.10.2/24`), enable `ip_forward` + NAT into LAN.
4. **Install WireGuard on Win11** client, set peer endpoint = `nyx.omnitec.net:51820` .
5. **Test** with `ping 192.168.1.x` , access `\\host\share` , and RDP.

🔑 Key Handling

- **Linux:** reference keys by filename in configs (`/etc/wireguard/keys/private.key`).
- **Windows:** paste private key inline (WireGuard stores it securely).
- **Public keys only** are exchanged between peers.

🔐 Security Benefits

- No raw SMB exposed to Internet.
- Encrypted in transit.
- Peer authentication per device.
- Least-privilege routing with `AllowedIPs`.

✅ Result

Remote users get **seamless, secure SMB access** as if they were in the office —
while keeping the office LAN safe from Internet threats.