MR.PLANB FIELD GUIDE · PROXMOX VE

Remote Proxmox With Zero Inbound Access: Setup Guide

Options and a recommended blend for reaching a Proxmox host you cannot open ports to.

Updated **2026-10-29** · Full guide: www.mrplanb.com/blog/remote-proxmox-zero-inbound-access

> When a host sits behind someone else's network with outbound traffic only, the community blend is a WireGuard or Tailscale endpoint on a dedicated router, one reserved IP for the host, a private VNet behind it, an optional Cloudflare or Pangolin tunnel for browser access, and an IP-KVM with power control for when networking breaks.

0
inbound ports, no port forwarding

16 / 128GB
cores and RAM in the example host

500+ Mbps
WireGuard speed reported on a GL.iNet travel router

4
pieces of advice in the final blend

The setup and the constraint

- A friend hosts a machine with 16 cores and 128GB RAM and offers outbound traffic only.
- No port forwarding, no firewall exceptions, no opening port 8006.
- The first plan was OpenVPN on the Proxmox host back to a home VPN server. It works, but WireGuard was widely favored.

The options compared

Option	Strength	Watch out for
OpenVPN on the host	Works; many people do it	Not the favored choice today
WireGuard	Cleaner routing, better speeds, fewer headaches	Needs a stable endpoint
Dedicated router (MikroTik, GL.iNet)	Tunnel stays up when Proxmox misbehaves or reboots	One more device to place
Tailscale	Works with no inbound access; subnet router in a container	Some workplaces block it
Cloudflare Tunnel	Browser access via a URL like pve.example.com	You must trust Cloudflare
Pangolin	Self-hosted tunnel, an alternative to Cloudflare	You run and secure it yourself

The recommended blend

1. Put a WireGuard or Tailscale endpoint on a dedicated router at the remote site.
2. Give the Proxmox host a single reserved IP on their network.
3. Keep everything else behind a private VNet, NAT, or an OPNsense/pfSense VM.

4. Add a Cloudflare or Pangolin tunnel for browser access, with strong authentication.
5. Install a remote KVM with power control.

Before you ship the box

- [ ] VPN lives on a router, not only inside the hypervisor.
- [ ] Host has one reserved IP so VMs do not fill the friend's DHCP pool.
- [ ] Tunnel tested from outside: turn off Wi-Fi on your phone and connect over cellular.
- [ ] IPMI/iLO/DRAC reachable through the tunnel where available.
- [ ] PicoKVM, JetKVM, Waveshare board or similar IP-KVM with a power relay installed.
- [ ] Browser access protected by strong authentication.

Why a router, not the host

Lifeline outside the hypervisor
If the host crashes, the VPN that gives you access should not crash with it.

Survives updates
A router keeps the tunnel open during Proxmox updates and reboots.

Reaches out-of-band
Lets you reach IPMI/iLO/DRAC when things go sideways.

Good guest behavior
A NAT VNet keeps your VMs off the friend's LAN, with a home router that knows the remote VNet.

Sources and notes: Homelab community discussion on running a remote Proxmox server (summarized on the page) · Tailscale, WireGuard and Cloudflare Tunnel as discussed in the thread