

Reach Your Home Server From Outside

Behind CGNAT, a changing IP or a firewall that only lets 443 out: how to tell which one you have, which method fits, and the exact commands for DDNS, a WireGuard relay on a VPS, Cloudflare Tunnel or Pangolin, and wstunnel. Built from the project documentation and the vpnsmith.com guides.

01 First, find out what is blocking you

CHECK	WHAT IT TELLS YOU
Router admin page, WAN address	The address your ISP gave the router
<code>curl -4 ifconfig.me</code> from a home machine	The address the internet sees
Both are the same	You have a real public IPv4: port forwarding and DDNS can work
WAN address in 100.64.0.0/10 (100.64.x to 100.127.x)	CGNAT: this block is reserved for it (RFC 6598). Inbound connections never reach you
WAN address in 10.x , 172.16-31.x or 192.168.x	Double NAT: another router sits in front of yours (ISP box in router mode, or CGNAT)
Same address, but it changes every few days	Dynamic IP: DDNS is enough, no VPS required
From the outside network, only TCP 80/443 leave	You are fighting the network you connect from, not your home line: see section 06

Before you go on. A tunnel removes the open port, it does not authenticate anyone. Whatever you expose is reachable by whoever learns the hostname, and hostnames leak through Certificate Transparency logs as soon as a TLS certificate is issued. Put a login in front of every exposed service.

02 Pick the method

YOUR SITUATION	METHOD	WHAT YOU NEED
Real public IP, it changes	DDNS + port forward (section 03)	A hostname and an updater, no extra cost
CGNAT, you want a VPN back into your LAN	WireGuard relay on a VPS (section 04)	A small VPS with a public IPv4
CGNAT, you expose web apps, no server to run	Cloudflare Tunnel (section 05)	A domain on Cloudflare
CGNAT, web apps, no third party in the path	Pangolin on a VPS (section 05)	A small VPS, and its upkeep

YOUR SITUATION	METHOD	WHAT YOU NEED
Remote network only lets 443 out, or detects WireGuard	wstunnel in front of WireGuard (section 06)	A VPS, a domain, Caddy
Need it always up, home line is slow or unreliable	Host the service on the VPS itself	A VPS sized for the service

03 DDNS on a dynamic IP

1. Create a hostname at a DDNS provider (many routers have one built in).
2. Run the updater: the router's DDNS setting, or `ddclient` (or a small Docker updater) on a home machine.
3. Set a short TTL on the record, 60 to 300 seconds. With a TTL of 3600, resolvers may serve your old address for an hour after it moves.
4. Forward the port on the router, for WireGuard UDP 51820 to the server's LAN IP.
5. Use the hostname in every client: `Endpoint = home.example.com:51820`.
6. Test from mobile data, never from inside your LAN.

WireGuard resolves the hostname when the interface comes up, not continuously. After an IP change the client keeps sending to the old address; `wg-quick down wg0 && wg-quick up wg0` forces a fresh lookup.

04 WireGuard relay through a VPS (CGNAT)

The home server dials out to the VPS, so nothing needs to reach your home line. The VPS gets the public IP and forwards what you choose down the tunnel.

ON THE HOME SERVER, PEER SECTION

```
[Peer]
PublicKey = VPS_PUBLIC_KEY
Endpoint = VPS_PUBLIC_IP:51820
AllowedIPs = 10.8.0.1/32
PersistentKeepalive = 25
```

`PersistentKeepalive = 25` is not optional here: without it the CGNAT mapping expires and the VPS can no longer reach home.

ON THE VPS, FORWARD A PUBLIC PORT TO HOME

```
sysctl -w net.ipv4.ip_forward=1
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 443 -j DNAT --to-destination 10.8.0.2:443
iptables -t nat -A POSTROUTING -o wg0 -j MASQUERADE
```

Replace `eth0` with the VPS public interface (`ip route get 1.1.1.1` shows it), `10.8.0.2` with the home server's tunnel address. Make `ip_forward` permanent in `/etc/sysctl.d/`, and open the forwarded port in the VPS firewall.

SYMPTOM	LOOK AT
Works for a minute, then the VPS cannot reach home	PersistentKeepalive missing on the home side
Tunnel up, forwarded port times out	<code>sysctl net.ipv4.ip_forward</code> must print 1; DNAT on the wrong interface
Service sees every visitor as 10.8.0.1	Expected with MASQUERADE; use a reverse proxy with X-Forwarded-For if you need the client IP

05 Cloudflare Tunnel or Pangolin

QUESTION	CLOUDFLARE TUNNEL	PANGOLIN
Who owns the public endpoint	Cloudflare's edge	A VPS you rent and run
Who decrypts TLS	Cloudflare, in the usual setup	Your VPS
Cost	Free plan available	No licence, you pay the VPS
Maintenance	None on the endpoint	Updates, certificates, backup of the config
Limits to know	90 s TCP ACK timeout, 30 s keep-alive, 900 s proxy idle timeout (errors 522 and 520)	Those of your own VPS

Both open an outbound connection from home, so both work behind CGNAT. A reasonable split: Cloudflare Tunnel for public, cache-friendly pages, a self-hosted tunnel for documents, backups and admin panels.

06 wstunnel when only 443 gets out

wstunnel wraps WireGuard's UDP in a WebSocket over TLS, so a hotel or office firewall sees ordinary HTTPS. One binary for client and server (github.com/erebe/wstunnel/releases).

SERVER, ALONE ON PORT 443

```
wstunnel server --restrict-to localhost:51820 \
--restrict-http-upgrade-path-prefix LONG-RANDOM-SECRET wss://[:]:443
```

CLIENT

```
wstunnel client --http-upgrade-path-prefix LONG-RANDOM-SECRET \
-L 'udp://51820:localhost:51820?timeout_sec=0' wss://your.server.com:443
```

Then set `Endpoint = 127.0.0.1:51820` in the WireGuard client config.

SYMPTOM	LOOK AT
Tunnel drops after about 30 seconds of silence	?timeout_sec=0 missing: the UDP timeout defaults to 30 s
Slow compared to plain WireGuard	Lower the WireGuard MTU; with Cloudflare proxying the domain (orange cloud), try it unproxied
Connection loops when WireGuard sends all traffic	Add a static route to the server IP via your normal gateway
Anyone could use your server as a proxy	--restrict-to missing: always pin the destination

Behind a reverse proxy such as Caddy, the proxy must forward the path that starts with your secret prefix to wstunnel, and wstunnel then listens on a local `ws://127.0.0.1:PORT`.

07 Need a server for the relay?

A WireGuard relay, a Pangolin endpoint or a wstunnel server needs a machine with a stable public IPv4 that stays on around the clock. A tunnel needs very little CPU; what matters is that the machine keeps running and stays patched. Contabo Cloud VPS 4 is listed at about 5.50 EUR/month excluding VAT on a 24-month term (contabo.com, read on 20 October 2026; check the current price on the order page): [see Contabo Cloud VPS](#). Smaller option: HostPapa Unmanaged VPS Lite (1 core, 1 GB RAM, 25 GB NVMe, 4 TB transfer, root SSH) is listed at 2.95 USD/month on a 3-year term, then the regular rate (hostpapa.com, read on 28 October 2026): [see the HostPapa VPS offer](#). Both are affiliate links: vpnsmith.com earns a commission if you buy, at no extra cost to you.

Full walkthroughs: [Dynamic DNS for a self-hosted VPN](#) · [Pangolin vs Cloudflare Tunnel](#) · [wstunnel guide](#) · [VPN on a Synology or QNAP NAS](#) · [WireGuard config generator](#).

This sheet summarises the vpnsmith.com guides, RFC 6598, the Cloudflare documentation and the wstunnel README (October 2026). It was not produced from a test bench across every ISP and network.