La VPN di casa con WireGuard

Guida per il server di casa · ottobre 2026 · vale per Agenda di Casa e per tutte le app che metterai sul tuo server

Riquadri: verde = messaggio per l'assistente IA · rosso = ATTENZIONE · giallo = NON PROVATO (come leggerli)

Questa guida ti fa raggiungere il server di casa **da fuori casa**, dal telefono o dal portatile, **senza aprirlo a internet**.

Lo strumento si chiama **VPN** (rete privata virtuale): un tunnel cifrato tra il tuo telefono e la rete di casa. Quando il tunnel è acceso, per il telefono è come essere a casa, anche se sei al mare. Useremo **WireGuard**, una VPN libera, moderna e leggera, con **wg-easy**, un pannello web che la rende semplice da gestire.

Perché una VPN e non "aprire il server"? Si potrebbe aprire il server direttamente a internet, ma allora chiunque nel mondo potrebbe provare a entrarci, giorno e notte. Con la VPN su internet resta aperta una sola porta, quella di WireGuard, che **non risponde a nessuno** che non abbia una delle tue chiavi. Tutto il resto resta chiuso in casa.

Se usi un assistente IA (per esempio un chatbot)

Puoi caricare questa guida nel tuo assistente e farti accompagnare. Copia e incolla questo messaggio insieme alla guida:

"Guidami a creare la VPN di casa seguendo questa guida. Prima chiedimi che router ho (marca e modello) e quale operatore internet uso. Poi guidami un passo alla volta: dimmi dove devo andare o cosa scrivere, aspetta che ti dica cosa vedo prima di passare al passo successivo, e confrontalo con 'Cosa deve succedere'. Se al passo 1 risulta che sono dietro CGNAT, fermati e spiegami le alternative. Non chiedermi mai di scriverti password, token o chiavi."

Come funziona, in parole semplici

1. Il **telefono**, fuori casa, accende il tunnel WireGuard.
2. Il tunnel va su internet verso **il nome della tua casa** (per esempio `vpn.tuodominio.eu`), che punta all'indirizzo internet di casa tua.
3. Il **router** di casa riceve il tunnel su **una sola porta** (UDP 51820) e lo passa al **server**.
4. Sul server, **wg-easy** controlla la chiave del telefono e lo fa entrare nella rete di casa.
5. Da lì il telefono raggiunge le tue app come se fosse sul Wi-Fi di casa.

Per arrivarci servono quattro cose, una per passo: un **indirizzo internet vero** (passo 1), un **nome** che lo segua quando cambia (passo 2), **wg-easy** sul server (passi 3 e 4) e la **porta aperta sul router** (passo 5).

Cosa ti serve

- Il **server di casa** con **Docker**. Se hai seguito la Strada 2 o 3 della guida di Agenda di Casa ce l'hai già; se hai seguito la Strada 1, installalo con il passo 2.1 di quella guida.
- L'**accesso alla pagina di gestione del router**: come entrarci e come farti guidare dall'IA sul tuo modello è spiegato nella guida Il router di casa.
- Per il passo 2, la strada consigliata: un **dominio** tuo (pochi euro all'anno) e un account gratuito su **deSEC**.
- Un **telefono** (e, se vuoi, un portatile) da collegare.
- Circa **un'ora e mezza** la prima volta. Puoi fermarti alla fine di ogni passo e riprendere un altro giorno.

Due cose da sapere sul terminale

Come nella guida di Agenda di Casa: il terminale si apre con **Ctrl+Alt+T**; si incolla con **Ctrl+Shift+V** o con **tasto destro → Incolla**; le password non si vedono mentre le scrivi; **copia i comandi dalla versione online** della guida, non dal PDF.

Se un comando incollato compare con caratteri in più all'inizio o alla fine (per esempio `[200~` o `00~`), **non premere Invio**: cancella la riga con **Ctrl+U** e incolla con **tasto destro → Incolla**.

Percorso rapido (per chi sa già come si fa)

1. Verifica di non essere dietro CGNAT: l'IP WAN del router deve coincidere con `curl -4 -s https://ifconfig.me`.
2. Un nome DNS che segue l'IP: dominio tuo con DNS su deSEC e aggiornamento ogni 10 minuti via `update.dedyn.io` (script del passo 2A), oppure il DDNS del router.
3. wg-easy v15 con Docker Compose (file del passo 3), pannello legato all'IP di casa del server, `INSECURE=true` solo perché il pannello non esce dalla rete di casa.
4. Procedura guidata su `http://IP-DEL-SERVER:51821`: amministratore, host = il tuo nome DNS, porta 51820. DNS dei client: `9.9.9.9`.
5. Router: inoltra **solo** UDP 51820 verso il server. Mai la porta 51821 né le porte delle app.
6. Un client per dispositivo; prova con i dati mobili.

Passo 1 — Hai un indirizzo internet "vero"? (controllo del CGNAT)

Questo è il controllo più importante: **fallo prima di tutto il resto**.

Molti operatori, per risparmiare indirizzi, mettono più clienti dietro lo **stesso** indirizzo internet. Si chiama **CGNAT**. Se sei in questa situazione, da internet nessuno può raggiungere casa tua, nemmeno il tuo telefono, e una VPN come questa **non può funzionare**. Meglio scoprirlo adesso che dopo un'ora di lavoro.

1. **L'indirizzo che vede internet.** Sul server:

```
curl -4 -s https://ifconfig.me; echo
```

Compare un numero come `93.40.12.7`. Annotalo.

1. **L'indirizzo che vede il router.** Entra nel router e leggi l'**indirizzo IP WAN**: guida Il router di casa, sezioni 2 e 5.1. Annotalo.

2. **Confronta:**

Risultato	Cosa vuol dire
I due numeri sono **uguali**	Hai un indirizzo vero. **Puoi continuare.**
Il numero del router inizia con **100.** (da 100.64 a 100.127)	Sei dietro **CGNAT**. Fermati: vedi sotto.
Il numero del router inizia con **10.**, **172.** o **192.168.**	C'è un secondo apparecchio tra router e internet (un altro modem). Prova a mettere il modem dell'operatore in modalità "bridge", oppure chiedi aiuto all'assistenza.
Sono diversi in un altro modo	Probabilmente CGNAT: chiedi conferma all'operatore.

Se sei dietro CGNAT: chiama l'operatore e chiedi un **indirizzo IPv4 pubblico** (a volte si chiama "IP pubblico" o "uscita dal NAT"). Alcuni operatori lo danno gratis su richiesta, altri a pagamento, altri non lo danno affatto. Senza indirizzo pubblico questa guida non fa per te: esistono alternative (un piccolo server in affitto che fa da ponte), ma sono più complesse e non sono trattate qui.

NON PROVATO da chi ha scritto la guida: la strada con CGNAT

Chi ha scritto la guida ha un indirizzo pubblico, quindi questo caso non l'ha vissuto. Prima di chiamare l'operatore, una seconda verifica: il sito natchecker.com/it spiega in italiano come controllare il CGNAT in più modi. Poi segnala cosa non ha funzionato (e cosa ha funzionato) scrivendo al progetto (proactiveproject.eu/progetto): così la guida migliora per tutti.

ATTENZIONE — l'indirizzo internet di casa cambia

Quasi sempre l'indirizzo che hai appena annotato **cambia ogni tanto** (dopo un riavvio del router o ogni qualche giorno). Per questo non lo scriveremo da nessuna parte: useremo un **nome** che lo segue da solo (passo 2).

Passo 2 — Un nome per la tua casa

Il telefono deve sapere dove trovare casa tua anche quando l'indirizzo cambia. Serve un **nome** (per esempio `vpn.tuodominio.eu`) che punti sempre all'indirizzo di oggi. Questo servizio si chiama **DDNS** (DNS dinamico).

Due strade:

	2A — Dominio tuo + deSEC (consigliata)	**2B — DDNS del router**
Costo	pochi euro all'anno per il dominio	di solito gratis
Da chi dipendi	solo da te (e dal rinnovo del dominio)	dal produttore del router e dal servizio scelto
Cosa impari	come funzionano davvero domini e DNS	poco: fa tutto il router
In più	lo stesso dominio serve per l'https, se un giorno vorrai	—

Perché la guida consiglia la 2A. I servizi di nomi gratuiti possono cambiare le condizioni o chiudere da un giorno all'altro (nel 2026 deSEC ha sospeso i suoi nomi gratuiti `dedyn.io`). Un dominio tuo resta tuo finché lo rinnovi. E capire come funziona un dominio è una competenza che ti servirà per tutto il resto.

2A — Dominio tuo + deSEC

deSEC è un servizio di DNS europeo (Berlino), senza scopo di lucro e gratuito: gestisce i nomi del tuo dominio e accetta gli aggiornamenti automatici dell'indirizzo.

2A.1 — Compra un dominio. Da un "registrar" (la società che vende i domini), meglio europeo. Per esempio INWX, quello usato da chi ha scritto questa guida.

- Scegli un nome semplice, magari con `.eu` o `.it`.
- **Guarda il prezzo di rinnovo**, non solo quello del primo anno: alcuni registrar fanno sconti il primo anno e poi costano molto di più.
- Attiva il **rinnovo automatico** e tieni aggiornato il metodo di pagamento: se il dominio scade, la VPN smette di funzionare.

2A.2 — Crea l'account su deSEC e aggiungi il dominio. Su desec.io crea un account, poi **Domain Management** → **+** → scrivi il tuo dominio (per esempio `tuodominio.eu`).

2A.3 — Fai gestire il dominio a deSEC (nameserver). Nella pagina del tuo dominio sul sito del registrar cerca **Nameserver** (o "Server DNS"). Sostituisci quelli che ci sono con i due di deSEC indicati nella pagina del dominio su deSEC (di solito `ns1.desec.io` e `ns2.desec.org`) e salva.

Il cambio può richiedere da qualche minuto a qualche ora. Nel frattempo puoi andare avanti.

Facoltativo ma consigliato — DNSSEC. È una "firma" che impedisce a qualcuno di falsificare i nomi del tuo dominio. deSEC te la prepara: nella pagina del dominio su deSEC trovi i dati **DS**, da copiare nella sezione **DNSSEC** del registrar. Se ti sembra troppo, puoi farlo più avanti.

2A.4 — Crea un "token" per gli aggiornamenti. Il **token** è una specie di password usata solo dallo script che aggiorna l'indirizzo. Su deSEC: **Token Management** → **+** → nome, per esempio `ddns-casa` → crea.

> **ATTENZIONE — il token si vede una volta sola**
>
> Copialo subito nel tuo gestore di password. Non scriverlo in chat, in email o in un'assistente IA. Se lo perdi, ne crei un altro e cancelli il vecchio.

2A.5 — Lo script che aggiorna l'indirizzo. Sul server.

Prima la cartella e il file del token (`chmod 700` e `600` vogliono dire "solo io posso leggerli"):

```
mkdir -p ~/ddns && chmod 700 ~/ddns && nano ~/ddns/token
```

Si apre l'editor **nano**: incolla il token (tasto destro → Incolla), poi **Ctrl+O**, **Invio** per salvare, **Ctrl+X** per uscire. Poi:

```
chmod 600 ~/ddns/token && wc -c ~/ddns/token
```

Cosa deve succedere: un numero (la lunghezza del token, più uno per il fine riga) e il nome del file. Il token non viene mostrato.

Ora lo script. **Prima di incollarlo** cambia `vpn.TUO-DOMINIO` con il nome vero (per esempio `vpn.tuodominio.eu`), poi incolla il blocco tutto intero:

```
cat > ~/ddns/aggiorna.sh <<'EOF'
#!/bin/sh
NOME="vpn.TUO-DOMINIO"
TOKEN=$(cat "$HOME/ddns/token")
IP=$(curl -4 -s --max-time 20 https://ifconfig.me)
VECCHIO=$(cat "$HOME/ddns/ultimo_ip" 2>/dev/null)
[ -z "$IP" ] && exit 0
[ "$IP" = "$VECCHIO" ] && exit 0
curl -4 -fsS --user "$NOME:$TOKEN" "https://update.dedyn.io/?
hostname=$NOME&myipv4=$IP&myipv6=preserve" && echo "$IP" > "$HOME/ddns/ultimo_ip"
EOF
```

Cosa fa lo script, riga per riga: legge il token dal suo file, chiede a internet "che indirizzo ho?", e **solo se è cambiato** lo comunica a deSEC, poi si segna l'ultimo indirizzo comunicato.

Prova:

```
sh ~/ddns/aggiorna.sh; echo
```

Cosa deve succedere: compare `good`. Se lo lanci una seconda volta non scrive niente: è normale, vuol dire "l'indirizzo non è cambiato, non disturbo deSEC". Se compare un errore `401`, il token non è giusto o il nome non è scritto come su deSEC.

Ora fallo girare da solo ogni 10 minuti:

```
(crontab -l 2>/dev/null; echo "*/10 * * * * sh $HOME/ddns/aggiorna.sh > /dev/null
2>&1") | crontab - && crontab -l
```

Cosa deve succedere: l'ultima riga mostrata è quella con `*/10 * * * *` e `aggiorna.sh`.

Controllo finale (dopo qualche minuto):

```
ping -c 1 vpn.TUO-DOMINIO
```

Cosa deve succedere: nella prima riga, tra parentesi, compare **lo stesso indirizzo** del passo 1. Non importa se poi il ping non riceve risposta: conta solo il numero tra parentesi.

2B — Il DNS dinamico del router

Molti router hanno una funzione **DDNS** o **DNS dinamico**: per trovarla sul tuo modello usa la frase per l'IA della guida Il router di casa, sezione 5.5. Funziona così:

1. Il router mostra un elenco di servizi supportati: scegline uno (per esempio dynv6, No-IP, DynDNS o il servizio del produttore del router, come MyFRITZ! per i Fritz!Box).
2. Crea un account su quel servizio e un nome (per esempio `casamia.dynv6.net`).
3. Scrivi nel router nome, utente e password (o token) del servizio, e salva.
4. Controlla dopo qualche minuto con `ping -c 1 IL-TUO-NOME` dal server (vedi il controllo finale della 2A).

> **NON PROVATO da chi ha scritto la guida**
>
> La strada 2B non è stata provata (le funzioni DDNS cambiano molto da router a router). Se qualcosa non torna: cerca "DDNS" nel **manuale del tuo router** o nella guida del tuo operatore, e controlla le istruzioni del servizio scelto. Se non ne esci, la strada 2A funziona con qualsiasi router. Poi segnala cosa non ha funzionato (e cosa ha funzionato) scrivendo al progetto (proactiveproject.eu/progetto): così la guida migliora per tutti.

Leggi le condizioni del servizio che scegli: alcuni servizi gratuiti chiedono di confermare il nome ogni mese, altrimenti lo cancellano.

Passo 3 — Installa wg-easy sul server

Ti serve l'**indirizzo di casa del server** (passo 1.7 della guida di Agenda di Casa, comando `hostname -I`, per esempio `192.168.1.10`).

Prima la cartella:

```
mkdir -p ~/wg-easy && cd ~/wg-easy && pwd
```

Poi il file di Docker. **Prima di incollarlo** cambia `IP-DEL-SERVER` con l'indirizzo di casa del server (per esempio `192.168.1.10`), poi incolla il blocco tutto intero:

```
cat > ~/wg-easy/docker-compose.yml <<'EOF'
services:
  wg-easy:
    image: ghcr.io/wg-easy/wg-easy:15
    container_name: wg-easy
    environment:
      - INSECURE=true
      - DISABLE_IPV6=true
    volumes:
      - ./dati:/etc/wireguard
      - /lib/modules:/lib/modules:ro
    ports:
      - "51820:51820/udp"
      - "IP-DEL-SERVER:51821:51821/tcp"
    cap_add:
      - NET_ADMIN
      - SYS_MODULE
    sysctls:
      - net.ipv4.ip_forward=1
      - net.ipv4.conf.all.src_valid_mark=1
    restart: unless-stopped
EOF
```

Le righe importanti, spiegate:

- `51820:51820/udp` è la porta del tunnel, l'unica che aprirai sul router.
- `IP-DEL-SERVER:51821:51821/tcp` è il **pannello** di wg-easy, raggiungibile **solo** dall'indirizzo di casa del server. Anche se un giorno sbagliassi qualcosa sul router, il pannello non sarebbe raggiungibile da internet.
- `INSECURE=true` permette di aprire il pannello senza https. Va bene **solo perché** il pannello resta dentro casa.
- `./dati` è la cartella con le chiavi e la configurazione: è da includere nelle copie di sicurezza.
- `restart: unless-stopped` fa ripartire wg-easy da solo dopo ogni riavvio.

Avvia:

```
cd ~/wg-easy && sudo docker compose up -d && sudo docker ps
```

Cosa deve succedere: nell'elenco compare `wg-easy` con stato `Up …`.

Passo 4 — La prima configurazione di wg-easy

1. Da un computer di casa apri il browser su `http://IP-DEL-SERVER:51821` (per esempio `http://192.168.1.10:51821`).
2. Si apre una **procedura guidata**. Crea l'**utente amministratore** del pannello: nome e password lunga, da salvare subito nel gestore di password.
3. Quando chiede l'**host** (l'indirizzo con cui i dispositivi trovano casa tua), scrivi **il nome del passo 2** (per esempio `vpn.tuodominio.eu`), **non** l'indirizzo numerico che cambia. Porta: **51820**.
4. Finita la procedura, vai in **Admin** → **Config** (impostazioni) → **DNS** e scrivi `9.9.9.9` (Quad9: un servizio di nomi europeo, senza pubblicità e attento alla privacy). Salva.

> **NON PROVATO passo per passo da chi ha scritto la guida**
>
> wg-easy è in uso sul server dell'autore, ma la procedura guidata qui sopra non è stata ricontrollata schermata per schermata, e può cambiare tra una versione e l'altra. Se una voce non corrisponde, segui la documentazione ufficiale di wg-easy: wg-easy.github.io/wg-easy. Le due cose da non sbagliare restano: come **host** il **nome** del passo 2 (non l'indirizzo numerico), e la porta **51820**. Poi segnala cosa non ha funzionato (e cosa ha funzionato) scrivendo al progetto (proactiveproject.eu/progetto): così la guida migliora per tutti.

Cosa deve succedere: entri nel pannello, con l'elenco dei dispositivi (client) ancora vuoto.

Passo 5 — Apri sul router una sola porta

Ora diciamo al router: "se arriva qualcosa sulla porta UDP 51820, passalo al server".

Segui la guida Il router di casa, sezione **5.3**: c'è la frase pronta da dare al tuo assistente IA, con le regole di sicurezza già dentro. La regola da creare è una sola:

Campo	Valore
Protocollo	**UDP**
Porta esterna	**51820**
Porta interna	**51820**
Dispositivo (indirizzo interno)	l'indirizzo di casa del server (per esempio `192.168.1.10`)

ATTENZIONE — solo questa porta, nient'altro

Non inoltrare **mai** la porta 51821 (il pannello di wg-easy), né le porte delle app (per esempio 8090), né la 22 (SSH), né la 80 o la 443. Spegni anche l'**UPnP** del router (guida Il router di casa, sezione 5.4): è una funzione che permette ai programmi di aprire porte da soli, senza chiederti niente.

Assicurati anche che l'indirizzo del server sia **prenotato** nel router (guida Il router di casa, sezione 5.2): se cambiasse, la porta verrebbe inoltrata al dispositivo sbagliato.

Passo 6 — Collega il telefono

Un dispositivo, un client. Ogni telefono e ogni portatile ha il suo collegamento personale. Non usare mai lo stesso su due dispositivi: si "rubano" il tunnel a vicenda e la connessione cade continuamente.

1. Nel pannello di wg-easy tocca **+ New** (nuovo client) e dagli un nome chiaro, per esempio `telefono-mario`. Crea.
2. Sul telefono installa un'app WireGuard:
   - **WireGuard** (l'app ufficiale) dal Play Store, oppure
   - **WG Tunnel** da F-Droid, libera e senza Google.
3. Nell'app tocca **+** → **Scansiona codice QR**.
4. Nel pannello di wg-easy, accanto al client appena creato, tocca l'icona del **codice QR** e inquadralo con il telefono.
5. Dai un nome al tunnel (per esempio `casa`) e salva. Android chiede il permesso di creare una VPN: **OK**.

Per un portatile Ubuntu: nel pannello crea un client apposta (per esempio `portatile-mario`) e scarica il **file** `.conf` invece del QR. Rinominalo con un nome corto, **massimo 15 caratteri** (per esempio `vpn-casa.conf`), poi importalo:

```
nmcli connection import type wireguard file ~/Scaricati/vpn-casa.conf && nmcli
connection modify vpn-casa connection.autoconnect no
```

Da quel momento lo accendi e spegni dal menu in alto a destra di Ubuntu.

Passo 7 — La prova vera, da fuori casa

Finché sei sul Wi-Fi di casa non puoi sapere se la VPN funziona davvero. Simula di essere fuori:

1. Sul telefono **spegni il Wi-Fi** e usa i **dati mobili**.
2. Nell'app WireGuard **accendi** il tunnel `casa`.

3. Apri l'app di casa (per esempio Agenda di Casa) oppure, nel browser, l'indirizzo di un'app del server (per esempio `http://192.168.1.10:8090/_/`).

Cosa deve succedere: l'app si collega come se fossi a casa.

L'app WireGuard può dire "collegato" anche quando non funziona: la prova vera è che **l'app di casa risponda**.

Le regole d'uso

Regola	Perché
Fuori casa: tunnel acceso. A casa: tunnel spento.	Con molti router, a tunnel acceso dentro casa il server non si raggiunge.
Un client per dispositivo	Due dispositivi con lo stesso client si tolgono il collegamento a vicenda.
Su Android funziona una sola VPN alla volta	Se usi un'altra VPN, spegnila prima di accendere quella di casa.
Se cambi il DNS nel pannello, va cambiato su ogni dispositivo	Il DNS viene copiato nel collegamento al momento della creazione.
Un telefono perso o rubato: cancella subito il suo client dal pannello	Da quel momento quel telefono non può più entrare.

Copie e aggiornamenti

- **Copia:** la cartella `~/wg-easy/dati` contiene la configurazione e le chiavi. Includila nelle copie di sicurezza del server. Senza, se il server si rompe, dovrai ricreare tutti i client.
- **Aggiornare wg-easy** (ogni tanto, leggendo prima le note della nuova versione):

```
cd ~/wg-easy && sudo docker compose pull && sudo docker compose up -d
```

Se qualcosa non va

Cosa succede	Cosa fare
Fuori casa il tunnel risulta "collegato" ma le app non rispondono	Controlla in ordine: 1) il nome punta all'indirizzo giusto (`ping -c 1 vpn.TUO-DOMINIO` dal server e confronto con il passo 1); 2) la regola sul router (UDP, 51820, indirizzo del server giusto); 3) `sudo docker ps` mostra `wg-easy` acceso; 4) l'indirizzo internet di casa non è passato sotto CGNAT (passo 1).
A casa, con il tunnel acceso, il server non si raggiunge	Normale con molti router: a casa spegni il tunnel.

Cosa succede	Cosa fare
La connessione cade ogni pochi minuti	Due dispositivi usano lo stesso client: creane uno per ciascuno.
Il tunnel non trova il nome (errore di risoluzione)	Il DDNS non sta aggiornando: `sh ~/ddns/aggiorna.sh` deve rispondere `good` (o niente, se l'indirizzo non è cambiato); controlla `crontab -l`.
Lo script risponde `401`	Token sbagliato o scaduto, oppure il nome nello script non è identico a quello su deSEC.
Il pannello `http://IP-DEL-SERVER:51821` non si apre	Sei sulla rete di casa? L'indirizzo nel file è quello giusto del server? `sudo docker logs --tail 20 wg-easy` mostra il motivo.
Il dominio è scaduto	Rinnovalo dal registrar: dopo il rinnovo tutto riprende da solo.

Licenze

WireGuard, wg-easy, deSEC e le app WireGuard citate sono software libero o servizi senza scopo di lucro. Questa guida fa parte del progetto ProactiveProject: se trovi un errore o un passo poco chiaro, scrivi al progetto.

Testo di questa guida: licenza CC BY-SA 4.0. Puoi copiarlo, tradurlo e modificarlo, anche per pubblicarlo altrove, citando **proactiveproject** e mantenendo la stessa licenza. **Una richiesta, non un obbligo:** se migliori la guida, proponi la modifica scrivendo al progetto (proactiveproject.eu/progetto), così il miglioramento arriva a tutti.