5.) Zugriff von unterwegs

Weboberfläche, App und Benachrichtigungen funktionieren auch außerhalb des Heimnetzes, ohne VPN: über `https://netmon.familieborghoff.de` (Monitor) und `https://ntfy.familieborghoff.de` (Benachrichtigungen).

```
Handy (Mobilfunk) ──https──▶ FritzBox :443 ──▶ Nginx Proxy Manager (Unraid) ──http──▶ Monitor 192.168.178.207:8085
```

Der Monitor selbst bleibt im Heimnetz auf Port 8085. Von außen erreichbar ist nur der Proxy, und nur über HTTPS.

Schutz

- **Anmeldesperre:** Nach 5 falschen Passwörtern in 15 Minuten wird der Absender 15 Minuten gesperrt. Hinter dem Proxy zählt die echte Adresse des Absenders. Das Heimnetz ist davon nicht betroffen.
- **Protokoll:** Jeder Fehlversuch steht im Container-Log als „Anmeldung fehlgeschlagen von …“ (geeignet für fail2ban).
- **Ersteinrichtung nur im Heimnetz:** Solange das Standardpasswort gilt, lässt sich das eigene Passwort nicht über den Proxy setzen.
- **Keine API-Beschreibung:** `/docs`, `/redoc` und `/openapi.json` sind abgeschaltet.

Das Passwort der Weboberfläche ist der einzige Schutz vor dem Sperren-Knopf. Es sollte lang und zufällig sein (mindestens 16 Zeichen) und nirgends sonst verwendet werden.

1. Adresse

`netmon.familieborghoff.de` muss auf die öffentliche IP des Anschlusses zeigen (DynDNS). Hinweis: Mit DS-Lite (keine eigene öffentliche IPv4) geht die IPv4-Portfreigabe nicht. Das zeigt die FritzBox unter *Internet → Online-Monitor*.

2. Portfreigabe in der FritzBox

Internet → Freigaben → Portfreigaben → Gerät für Freigaben hinzufügen → Unraid (192.168.178.207):

Extern	Intern	Wofür
TCP 443	HTTPS-Port des Nginx Proxy Manager	Zugriff
TCP 80	HTTP-Port des Nginx Proxy Manager	nur für das Let's-Encrypt-Zertifikat

Port 8085 (Monitor) und 8091 (ntfy) werden **nicht** freigegeben, beide laufen nur über den Proxy. Nutzt der FritzBox-Fernzugang selbst Port 443 (*Internet → Freigaben → FRITZ!Box-Dienste*), muss er auf einen anderen Port.

3. Proxy-Host im Nginx Proxy Manager

Hosts → Proxy Hosts → Add Proxy Host:

- Domain `netmon.familieborghoff.de`
- Scheme `http`, Forward Hostname `192.168.178.207`, Port `8085`
- *Block Common Exploits* an
- Reiter SSL: Let's-Encrypt-Zertifikat, *Force SSL* und *HSTS* an

Keine Access List mit Benutzer und Passwort davorschalten. Monitor und App melden sich selbst per Basic Auth an, eine zweite Abfrage am Proxy würde die App aussperren.

4. Monitor und App einstellen

- Weboberfläche → *Einstellungen* → „Adresse dieser Weboberfläche (für Links in Nachrichten)“: `https://netmon.familieborghoff.de/`. Dann führen die Links in den Benachrichtigungen auch unterwegs zum Gerät.
- App → *Einstellungen* → *Verbindung*:
  - Adresse im Heimnetz: `http://192.168.178.207:8085`
  - Adresse unterwegs: `https://netmon.familieborghoff.de`

  Die App probiert zuerst die Adresse, die zuletzt funktioniert hat, und weicht bei Bedarf auf die andere aus. Unterwegs dauert die erste Anfrage deshalb ein paar Sekunden länger.

5. Prüfen

Mit dem Handy im Mobilfunk (WLAN aus):

- `https://netmon.familieborghoff.de` öffnet die Anmeldung, das Zertifikat ist gültig.
- `https://ntfy.familieborghoff.de` zeigt die ntfy-Seite, Themen lassen sich nur nach Anmeldung lesen.
- Die öffentliche IP mit Port 8085 ist **nicht** erreichbar.
- Fünfmal ein falsches Passwort: danach meldet die Seite „Zu viele falsche Passwörter“.

6. Benachrichtigungen unterwegs (ntfy)

ntfy ist mit Anmeldepflicht eingerichtet (siehe Neuinstallation, Schritt 2): Ohne Benutzer kann niemand mitlesen oder Nachrichten schicken.

1. **Proxy-Host** im Nginx Proxy Manager:
   - Domain `ntfy.familieborghoff.de`
   - Scheme `http`, Forward Hostname `192.168.178.207`, Port `8091`
   - *Websockets Support* an, *Block Common Exploits* an
   - SSL: Let's-Encrypt-Zertifikat, *Force SSL* und *HSTS* an
2. **Monitor:** Einstellungen → ntfy: Server `https://ntfy.familieborghoff.de`, Thema `netzwerkmonitor`, Zugriffstoken des Benutzers `netzwerkmonitor`. (Bei Jans Installation steht das Token als `NTFY_TOKEN` in der `.env`.)
3. **ntfy-App:**
   - Einstellungen → *Benutzer verwalten* → Server `https://ntfy.familieborghoff.de`, Benutzer `jan`
   - Thema `netzwerkmonitor` auf diesem Server abonnieren
   - altes Abo auf `http://192.168.178.207:8091` löschen
4. **Test:** In der Weboberfläche „Testnachricht senden“, am besten mit dem Handy im Mobilfunk.

Echte Meldungen zu neuen Geräten öffnen beim Antippen direkt die Netzwerkmonitor-App mit dem Gerät (`netmon://device/…`), ohne Umweg über den Browser.

Neuen ntfy-Benutzer oder neues Token anlegen (Unraid-Terminal):

```
docker exec -it ntfy ntfy user add --role=admin jan
docker exec -it ntfy ntfy token add netzwerkmonitor
docker exec -it ntfy ntfy user list
```

Revision #2
Created 29 October 2026 14:23:26 by Jan
Updated 29 October 2026 14:54:26 by Jan