

BE services & infrastructure — validation map

From 20260608_BE_SERVICES_and_infra.md

Table of contents

[Topology](#)

[Service inventory \(mobile + console\)](#)

[Data paths](#)

[Cast session \(LAN — alpha scope\)](#)

[Telemetry path](#)

[Remote access control plane](#)

[Validation status](#)

[DNAT chain \(WireGuard lab\)](#)

[RSSH / RBAC](#)

[Planned: SFU relay \(Janus-class\)](#)

[Agent scripts](#)

[Open findings → tickets](#)

Source: 20260608_BE_SERVICES_and_infra.md — section links work in PDF viewers that support internal anchors.

Topology

```
flowchart LR
    subgraph Internet
        MOB["■ Android app"]
        OPS["■ Operator browser"]
    end

    subgraph Router["f0xx.org router"]
        RDNAT["UDP 45340 DNAT"]
    end

    subgraph FE["FE f0xx-monstro · apps.f0xx.org"]
        TLS["TLS :443"]
        FEDNAT["UDP 45340 DNAT"]
        NGXFE["nginx reverse proxy"]
    end

    subgraph BE["BE Alpine artc0 · :80"]
        NGXBE["nginx apps.conf"]
        FPM["PHP-FPM"]
        DB["MariaDB / SQLite"]
        WG["wg0 :45340"]
        SSH["sshd bastion :443"]
    end

    MOB -->|"HTTPS crashes/graphs/heartbeat"| TLS
    OPS --> TLS
    TLS --> NGXFE --> NGXBE --> FPM --> DB
    MOB -->|"UDP WG lab"| RDNAT --> FEDNAT --> WG
    MOB -->|"RSSH outbound"| SSH
    FPM --> WG
```

Hop	Host	Role
Public DNS	apps.f0xx.org, ra.apps.f0xx.org	CNAME → FE
Router	f0xx.org (134.17.26.161 WAN)	UDP 45340 → FE 10.7.0.10
FE	Gentoo HVM	TLS, HTTP proxy → BE :80, UDP DNAT → BE 10.7.16.128
BE	Alpine 10.7.16.128	PHP consoles, device APIs, wg0, RSSH bastion

Service inventory (mobile + console)

Service	Public URL / port	Mobile uses	Console uses	Status
Hub	https://apps.f0xx.org/app/androidcast_project/	Indirect (links)	Landing	■ OK
Crashes console	.../crashes/	—	Reports, home	■ OK
Crash upload	.../crashes/api/upload.php	■ gzip JSON	—	■ OK
Heartbeat / RA	.../crashes/api/heartbeat.php	■ RA poll	—	■ OK
Session stats / graphs ingest	.../graphs/api/graph_upload.php	■ (when enabled)	—	■ OK
Graphs dashboard	.../graphs/	—	Analytics UI	■ OK
Tickets	.../crashes/?view=tickets	—	Issue tracking	■ OK
Remote access	.../crashes/?view=remote_access	—	WG/RSSH ops	■ OK
RBAC admin	.../crashes/?view=rbac	—	Roles / lockouts	■ OK
APK builder	.../build/	—	Internal builds	■ OK
OTA channel	.../v0/ota/channel/stable.json	■ settings.json	—	PENDING HTTP 400 — not on apps vhost
OTA manifest/APK	TBD host/path	■	—	PENDING align with device ota.base_url
Diag API	.../crashes/api/diag.php	Optional	—	■■ 403 at edge (use upload/heartbeat)
WireGuard data	ra.apps.f0xx.org:45340/udp	■ lab mode	—	■ DNAT chain + BE listen

RSSH bastion	ra.apps.f0xx.org:443 /tcp	■ alpha mode	Operator SSH	■ API connect payload
--------------	---------------------------	--------------	--------------	-----------------------

Data paths

Cast session (LAN — alpha scope)

Sender UDP/TCP :41235 ↔ Receiver :41235
Discovery UDP :41234 (+ NSD)

No BE required for LAN alpha.

Telemetry path

Phone → HTTPS → FE → BE PHP
upload.php crash JSON
heartbeat.php session + RA
graph_upload.php session metrics

Remote access control plane

Phone poll → heartbeat.php (type:ra)
Operator → remote_access.php (whitelist, open_session, dashboard)
BE → wg set / rssh session row → connect JSON on next poll

Validation status

Run: examples/crash_reporter/backend/scripts/validate_be_services.sh

Check	2026-06-08 result
Hub / crashes / graphs / build HTTP	■
JS syntax (app, graphs, tickets, i18n)	■
RBAC API smoke (on BE localhost)	■
RA API smoke	■ (BE)
RSSH API smoke	■ test_rssh_api.sh
OTA public URL	FAIL 400
Browser SyntaxError (historical)	■ cleared — deployed JS passes node --check

DNAT chain (WireGuard lab)

sequenceDiagram
participant M as Mobile / laptop
participant R as Router f0xx.org
participant F as FE monstro
participant B as BE wg0

M->>R: UDP 45340 (public)
R->>F: DNAT → 10.7.0.10:45340
F->>B: DNAT → 10.7.16.128:45340
B->>B: wg0 decrypt

Script	Host	Persist hook
wireguard_router_dnat.sh	f0xx.org /home/scripts/	iodine_warmup_helper.sh apply_rules
wireguard_fe_dnat.sh	f0xx-monstro	xen_firewall.sh start/stop
install_be_remote_access.sh	alpine-be	wg0 + sudoers

RSSH / RBAC

Component	Path	Tune on BE
RSSH sessions	sql/migrations/009_rssh_sessions.sql	MariaDB migrate
Provisioner	src/RsshSessionProvisioner.php	config.php → remote_access.rssh
Bastion	sshd / stream on :443	host keys, port range 18000-18999
RBAC API	api/rbac.php	privilege_sets, lockout clear
Cron purge	scripts/purge_remote_access.php	hourly crontab

Smoke: test_rssh_api.sh, test_rbac_api.sh, ra_e2e_cli.sh

Planned: SFU relay (Janus-class)

> **Not in alpha.** Gray = future design surface; implementation on branch feature/sfu-relay, hidden from users until spec lands.

```
flowchart TB
    classDef future fill:#e5e7eb,stroke:#9ca3af,color:#374151

    subgraph Future["SFU path (planned)"]
        SFU["Janus / mediasoup SFU<br/>BE :8089 or dedicated"]
        SIG["Signaling API<br/>PHP or sidecar"]
        TURN["TURN optional"]
    end

    subgraph Today["Alpha today"]
        LAN["LAN UDP/TCP cast"]
        RA["RSSH debug"]
    end

    MOB2["Android"] --> LAN
    MOB2 -->|"post-alpha"| SIG
    SIG --> SFU
    SFU --> TURN
    OPS2["Operator"] --> SIG

    class SFU,SIG,TURN future
```

Piece	Status	Branch / flag
CastConfig.SFU_RELAY_PREVIEW	Stub false	feature/sfu-relay
config.php → sfu.enabled	Stub false	BE
api/sfu_health.php	Returns disabled	BE
Android SfuRelayGate	Hidden dev compile gate	App
FE nginx location /janus/	Exists for other stack — do not mix with androidcast vhost	INFRA §8089
Nginx + UDP ports for WebRTC	Design TBD with owner spec	—
Mobile TRANSPORT_WEBRTC UI	Frozen (ALPHA_FEATURE_FREEZE)	—

When the owner spec arrives: wire signaling auth to existing session/RBAC, add SFU room lifecycle beside (not replacing) LAN cast, and extend this doc § with concrete ports and URLs.

Agent scripts

Script	Purpose
validate_be_services.sh	Public reachability + JS syntax
verify_remote_access_prod.sh	BE WG/RSSH preflight
test_rssh_api.sh	RSSH connect payload
test_rbac_api.sh	RBAC panel API
ra_e2e_cli.sh	Full RA operator+device flow
test_graphs_api.sh	Graph ingest + dashboard

Open findings → tickets

ID	Severity	Topic	Track in
SVC-OTA	High	OTA v0/ota returns 400 on apps.f0xx.org — wire nginx + staging path	Tickets dashboard
SVC-DIAG	Low	diag.php 403 at public edge	Issues (documented workaround)
SVC-URL	Medium	Legacy f0xx.org crash URL 404 — devices should use apps.f0xx.org	Tickets + device settings.json
SFU-SPEC	Planning	Owner SFU spec integration	Issues (gray / post-alpha)

File via crashes console → **Tickets** for service/URL/nginx work; **Issues** for infra validation notes and SFU planning.