

Чек-лист деплоя NAT, STUN, TURN

К статье «NAT, фаерволы, STUN, TURN, ICE: как WebRTC реально добирается до телефона»

1 · Порты и транспорты

Открыть каждый транспорт, который описан в спецификации, и проверить в проде.

- ☐ STUN: UDP/3478 открыт на вход и выход на каждом TURN-хосте.
- ☐ TURN: UDP/3478, TCP/3478, TLS поверх TCP/5349 — все доступны.
- ☐ turns://host:443 поверх TLS — универсальный fallback для корп. фаерволов.
- ☐ Проверить, что реальный клиент сначала пробует UDP и чисто откатывается на TLS/443.
- ☐ Заблокировать прямой egress с TURN-хоста, кроме как в публичный интернет.

2 · Учётки (RFC 8656 §9.2)

Короткоживущие HMAC-учётки, выпускаемые server-side под каждый звонок.

- ☐ Выпускать ephemeral usernames (например, unixtime:userid) на app-сервере.
- ☐ Считать пароль = `base64(HMAC-SHA1(username, shared_secret))`.
- ☐ Срок жизни учётки ≤ 24 ч, для чувствительных вертикалей — минуты.
- ☐ Регулярно ротировать shared secret TURN; держать N-1 окно перекрытия.
- ☐ Никогда не выкладывать долгоживущие учётки TURN в клиентский код или HTML.

3 · Географическое размещение

Задержка TURN = удвоенный RTT клиент-TURN.

- ☐ Деплоить хотя бы один TURN-кластер на каждый континент пользователей.
- ☐ Использовать anycast IP или geo-DNS, чтобы рулить клиентов в ближайший кластер.
- ☐ Целевой P75 RTT клиент-TURN — ≤ 40 мс в каждом регионе.
- ☐ Помнить про длинный хвост: сельская мобильная, Starlink, CGNAT добавят 80–120 мс.
- ☐ Ограничить срок allocation; реклаймить простаивающие слоты после ≤ 10 мин.

4 · KPI observability

Инструментируйте каждый звонок и каждую TURN-allocation; покажите дашборд.

- ☐ Доля connected ICE по типу сети (Wi-Fi / 4G / 5G / корпоративная).
- ☐ Доля TURN-релея — 15–20 % для consumer, ~100 % для AI / IoT.
- ☐ Медианное время до selected candidate — цель ≤ 500 мс с Trickle ICE.
- ☐ Трафик TURN на звонок = 2 × битрейт звонка.
- ☐ Сбои consent freshness (RFC 7675) — алертировать при 0,5 % падений сессий.

Расчёт TURN-трафика — 1000 одновременных звонков, 20 % релеящихся

200 релеящихся × 3,2 Мбит/с (1,6 Мбит/с × 2 направления) = 1,28 Гбит/с sustained на TURN. Месячный egress ≈ 410 ТБ при коэффициенте busy-hour 12,5 %.

Цена на AWS EC2 egress $\sim \$0,054/\text{ГБ}$ выше 150 ТБ: $\approx \$22\,000$ / месяц. Тот же поток на колокейшен bare-metal с транзитом $\$0,50\text{--}\$1,00$ за Мбит/с в месяц: $\approx \$700\text{--}\$1\,400$ / месяц. 20-кратная разница — причина, по которой WebRTC значимого масштаба идёт на bare-metal или к TURN-провайдеру с bare-metal-экономикой.

Контролирующие спецификации: RFC 8489 (STUN, фев 2020) · RFC 8656 (TURN, фев 2020) · RFC 8445 (ICE, июл 2018) · RFC 8838 (Trickle ICE, янв 2021) · RFC 4787 (поведение NAT) · RFC 7675 (consent freshness).