Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

IP-телефония офиса на Asterisk 22 + FreePBX 17: наша методика

Как мы строим офисную АТС: PJSIP-транспорт, контур анти-фрода, очереди, запись, связка с CRM

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Офису нужна телефония с очередями, записью и CRM, но облако при 15+ пользователях дорого, а «самодельный» Asterisk без защиты — это открытый 5060/UDP, гостевые вызовы и счёт за ночной фрод-трафик на сотни тысяч рублей. Мы разворачиваем АТС на Asterisk 22 LTS + FreePBX 17 со встроенным контуром анти-фрода, мониторингом и резервированием — и сопровождаем её в эксплуатации.

Почему это важно бизнесу

- Телефонный фрод: одна слабая учётка — и ночные исходящие на дорогие направления превращаются в счёт на сотни тысяч рублей
- Час простоя телефонии в отделе продаж — потерянные входящие лиды, которых нет ни в CRM, ни в списке пропущенных
- Облако при 25–30 пользователях дороже своей АТС уже на горизонте года: абонплата за каждого против фиксированного VPS
- Записи разговоров на своём сервере — контроль качества менеджеров и аргумент в спорах с контрагентами

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

22 LTS

Ветка Asterisk: только chan_pjsip (chan_sip удалён в 21-й), LTS — 4 года + год security-фиксов

по докам asterisk.org

17

FreePBX на Debian 12: ставим официальным скриптом sng_freepbx_debian_install.sh (~30 минут)

FreePBX 17 / Debian 12

5 / 24 ч

fail2ban jail asterisk: maxretry=5, bantime=86400 — брут SIP-регистраций гасим за минуты

наш стандарт

60 с

qualify_frequency транка и эндпоинтов: OPTIONS-пинг каждые 60 с — авария видна до жалоб людей

по докам Asterisk (PJSIP)

10000–20000

Диапазон RTP (rtpstart/rtpend в rtp.conf): в фаерволе открыт только он и только оператору

наш стандарт

DSCP EF/46

tos_audio=ef, cos_audio=5 — приоритет голоса в сети; без QoS «бульканье» уже при 6+ разговорах

по докам Asterisk

РЕАЛИЗАЦИЯ 1 ИЗ 3

Ядро АТС: Debian 12 → Asterisk 22 LTS → FreePBX 17 за один день

Что настраиваем

VPS 2 vCPU / 4 GB RAM / 60 GB SSD под офис до 40 SIP-абонентов; всё на PJSIP, без legacy chan_sip

Как мы это делаем

1. Чистый Debian 12 на VPS, затем официальный скрипт sng_freepbx_debian_install.sh — Asterisk 22 LTS, FreePBX 17, MariaDB и Apache одним прогоном за ~30 минут
2. PJSIP: сигнализацию уводим с 5060/UDP на нестандартный порт; для удалёнки отдельный transport protocol=tls (method=tlsv1_2) + SRTP (media_encryption=sdes)
3. NAT-блок транспорта: external_media_address, external_signaling_address, local_net — без них получаем классический «односторонний звук» из-за серого IP в SDP
4. Транк оператора: identify по IP его SBC, from_user=номер, qualify_frequency=60; RTP фиксируем в rtp.conf: rtpstart=10000, rtpend=20000
5. Финализация: fwconsole ma upgradeall и fwconsole reload; модуль Backup & Restore шлёт ночную копию конфигов и БД на внешний FTP

РЕЗУЛЬТАТ

Воспроизводимая установка: одна и та же связка версий на каждом внедрении, обновления безопасности прилетают штатно через apt и fwconsole, а восстановление АТС из бэкапа на чистый VPS занимает меньше двух часов — проверяем это тестовым прогоном при сдаче проекта.

КЛЮЧЕВОЙ НЮАНС

С Asterisk 21 драйвер chan_sip удалён из исходников — вся конфигурация только через res_pjsip. Старые мануалы с sip.conf в 2026 году вредны: сверяемся с разделом Configuring res_pjsip официальной доки.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Контур анти-фрода: чтобы ночью не «наговорили» на сотни тысяч

Что настраиваем

Периметр VPS + логика маршрутизации исходящих: закрываем и сеть, и диалплан одновременно

Как мы это делаем

1. Responsive Firewall FreePBX (iptables): SIP-порт открыт только подсетям оператора и офисному VPN, RTP-диапазон — только медиасерверам оператора
2. fail2ban по security-логу Asterisk (logger.conf: security_log => security, модуль res_security_log): maxretry=5, findtime=600, bantime=86400
3. В SIP Settings отключаем гостей: Allow SIP Guests = No, Allow Anonymous Inbound SIP Calls = No; на эндпоинтах max_contacts=1
4. Outbound Routes: международные префиксы закрыты по умолчанию, белый список направлений + PIN на маршрут для избранных
5. Ночной контроль CDR: скрипт по таблице cdr в MariaDB — всплеск исходящих x5 от нормы или нецелевая страна → алерт в Telegram

РЕЗУЛЬТАТ

Поверхность атаки сведена к подсетям оператора и VPN; перебор паролей гаснет на пятой попытке, а даже украденная учётка физически не может звонить на платные направления. Ночной фрод ловится алертом за минуты, а не счётом оператора в конце месяца.

КЛЮЧЕВОЙ НЮАНС

Нюанс по доке: fail2ban должен читать именно security-лог Asterisk (res_security_log), а не общий full — иначе часть событий InvalidPassword просто не матчится фильтром и брут остаётся невидимым.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Маршрутизация, запись разговоров и связка с CRM/1C

Что настраиваем

IVR, очереди отделов, запись, всплывающая карточка в Битрикс24 — на том же узле АТС

Как мы это делаем

1. IVR на 2–3 уровня + Time Conditions (рабочие часы, праздники); очереди отделов со strategy=rrmemory, таймаутом звонка и объявлением позиции
2. Запись: MixMonitor в wav49 (GSM, примерно в 10 раз компактнее PCM-wav), 90 дней на сервере, старше — архив на NAS клиента по rsync
3. AMI только на 127.0.0.1 (manager.conf, порт 5038), отдельный пользователь с правами read=call — коннектор ловит события для карточки CRM
4. Нормализация номеров в диалплане до E.164 (79XXXXXXXXX) — иначе Битрикс24 не находит контакт, записанный как «8-916-...»
5. Zabbix-мониторинг: статус регистрации транка (pjsip show registrations), активные каналы (core show channels count), место под записями

РЕЗУЛЬТАТ

Менеджер видит карточку клиента до снятия трубки, руководитель — очереди и пропущенные в отчётах, спорные ситуации решаются записью разговора. Диск не растёт бесконтрольно, а падение транка чинится до того, как его заметит первый звонящий.

КЛЮЧЕВОЙ НЮАНС

Интеграцию строим на событиях AMI и наружу его не публикуем: bind на loopback, минимальные права пользователя. Для сложных сценариев есть ARI, но для карточки CRM событий AMI достаточно.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **SIP ALG на роутере клиента**
  Keenetic/Mikrotik «чинят» SIP-заголовки и рвут регистрации. Отключаем ALG/sip helper на шлюзе, NAT решаем параметрами PJSIP-транспорта.

- ✕ **Односторонний звук за NAT**
  Забытые external_media_address и local_net: в SDP уходит серый IP. Прописываем внешние адреса в transport и перезагружаем res_pjsip.

- ✕ **Конфиги chan_sip при миграции**
  С Asterisk 21 chan_sip удалён — старый sip.conf мёртв. Переносим на pjsip заранее: nat=yes превращается в rtp_symmetric=yes + force_rport=yes.

- ✕ **Пароль экстеншена = его номер**
  Связки вида 1001/1001 сканеры перебирают за минуты. Только автогенерация FreePBX: случайный secret от 16 символов, у каждого свой.

- ✕ **Открытый 5060/UDP всему интернету**
  Порт находят сканеры за часы. Ограничиваем источники подсетями оператора и VPN, для остальных — Responsive Firewall в режиме rate-limit.

- ✕ **Международка открыта по умолчанию**
  Одна взломанная учётка — счёт на сотни тысяч. Закрываем префиксы 810/00 в Outbound Routes, белый список стран и дневной лимит минут.

- ✕ **Записи в wav вместо wav49**
  wav ест ~1 МБ/мин и забивает диск за месяцы. wav49 плюс ротация 90 дней и выгрузка архива на NAS снимают проблему навсегда.

- ✕ **Транк без qualify и мониторинга**
  Оператор молча падает — входящие теряются часами. qualify_frequency=60 плюс триггер Zabbix на статус регистрации транка.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Asterisk 22 LTS + FreePBX 17 на Debian 12, только PJSIP
- fail2ban: 5 попыток → бан на 24 ч, нестандартный SIP-порт
- Запрет международных направлений и анонимных вызовов
- Случайные пароли экстеншенов от 16 символов

НОРМАЛЬНО

- SIP-порт только с подсетей оператора и VPN, RTP 10000–20000
- TLS + SRTP для удалённых сотрудников и софтфонов
- Запись wav49, ротация 90 дней + архив на NAS клиента
- Ночной контроль CDR с алертом в Telegram при всплеске x5

ХОРОШО

- Резервный SIP-транк второго оператора + failover-маршруты
- Холодный резерв АТС: rsync конфигов, переключение ≤30 минут
- Zabbix: транк, каналы, диск, качество звука по RTCP
- QoS насквозь: DSCP EF на АТС + приоритетная очередь на роутере

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] SIP-порт закрыт от интернета и открыт только оператору и корпоративному VPN?
- [ ] fail2ban читает security-лог Asterisk и банит перебор регистраций?
- [ ] Международные направления закрыты, белый список и лимиты минут настроены?
- [ ] Пароли всех экстеншенов случайные, ни один не совпадает с номером?
- [ ] Есть алерт при аномальном росте исходящих звонков ночью и в выходные?
- [ ] Записи разговоров ротируются и не забьют диск через полгода?
- [ ] Резервная копия FreePBX уезжает на внешний узел по расписанию?
- [ ] Падение SIP-транка видно в мониторинге раньше, чем позвонит клиент?
- [ ] Удалённые сотрудники подключаются по TLS/SRTP, а не по открытому UDP?
- [ ] SIP ALG отключён на офисном роутере?

Если хотя бы на два вопроса ответ «нет» или «не знаю» — тема требует внимания.

ЧТО МЫ ДЕЛАЕМ

Как поможет ITFresh

ITFresh — ИТ-аутсорсинг для юридических лиц до 50 рабочих мест в Москве и области. 15+ лет практики, собственная инфраструктура в дата-центре МТС (8 серверов Dell Xeon Platinum).

- Разворачиваем АТС под ключ: VPS, Asterisk 22 + FreePBX 17, транк, IVR, очереди, запись — за 5–10 дней
- Строим контур анти-фрода: фаервол, fail2ban, лимиты направлений, ночной CDR-контроль с алертами
- Интегрируем с Битрикс24 и 1С: всплывающая карточка, клик-звонок, журнал звонков в CRM
- Берём на поддержку 24×7: Zabbix-мониторинг, обновления безопасности, бэкапы, квартальный аудит
- Мигрируем со старых АТС и chan_sip-конфигов на PJSIP без простоя рабочего дня

15+
лет в ИТ-поддержке

50
рабочих мест — наш профиль

МТС
дата-центр, Москва

КОНТАКТЫ

Обсудить вашу задачу

Сайт	**itfresh.ru**
Телефон	**+7 903 729-62-41**
Telegram	**@ITfresh_Boss**

Бесплатно посмотрим вашу инфраструктуру по этому чек-листу и скажем, где тонко — без обязательств.

itfresh.ru

ДОКУМЕНТАЦИЯ И НАШ СТЕК

Техническая база

01 Asterisk Versions — циклы поддержки LTS-веток (docs.asterisk.org — 22 LTS)

02 Configuring res_pjsip (transports, NAT, qualify) (docs.asterisk.org — 2026)

03 Important Security Considerations (docs.asterisk.org — 2026)

04 FreePBX 17 Installation (Debian 12) (sangomakb.atlassian.net — 17)

05 sng_freepbx_debian_install — официальный скрипт (github.com/FreePBX — 2026)

06 Шаблон ITfresh: контур анти-фрода офисной АТС (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.