Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Caddy или Nginx: как мы выбираем веб-сервер в 2026

Наши критерии выбора и эталонные конфигурации для сайтов малого бизнеса: TLS, HTTP/3, Битрикс

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Сайт клиента обычно живёт на дорогом shared-хостинге: сертификат продлевают руками, конфиг веб-сервера никто не понимает, падение замечают по звонку клиента. Бездействие кончается «небезопасным» замочком в браузере и лежащим сайтом в разгар рекламной кампании. Мы переводим такие сайты на VPS: статика и WordPress — Caddy 2.11, Битрикс и публикация 1С — nginx 1.30, плюс TLS, лимиты и мониторинг.

Почему это важно бизнесу

- Просроченный сертификат = «Не защищено» в браузере: заявки падают до нуля, пока инженер ищет, где живёт certbot
- Час простоя сайта в разгар рекламной кампании — слитый бюджет на клики и потерянные лиды
- Переплата 3000–4500 ₽/мес за «битрикс-хостинг» там, где хватает VPS за ~1000 ₽ с Caddy
- Конфиг, который понимает один подрядчик, — операционный риск: смена студии превращается в квест

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

2.11.4

Ветка Caddy, которую ставим на новые сайты: автопродление TLS и HTTP/3 из коробки

Caddy releases, 2026

1.30.3

Stable-ветка nginx для прода; mainline 1.31.x (нечётная) держим только на стендах

nginx.org, июнь 2026

1/3 срока

renewal_window_ratio: Caddy перевыпускает сертификат, когда осталась треть его срока

по докам Caddy, tls

30 дней

остаток срока, при котором certbot продлевает 90-дневный cert (правило 1/3 с 4.0); certbot.timer — проверка дважды в сутки

Certbot User Guide

TLS 1.2+

дефолт Caddy: min tls1.2, max tls1.3; на nginx прописываем ssl_protocols TLSv1.2 TLSv1.3 сами

доки Caddy / nginx

UDP 443

порт QUIC для HTTP/3: если фаервол пропускает только TCP, браузеры молча откатываются на HTTP/2

наш стандарт

РЕАЛИЗАЦИЯ 1 ИЗ 3

WordPress и статика: связка Caddy 2.11 + PHP-FPM

Что настраиваем

Типовые корпсайты и каталоги на VPS 2 vCPU / 4 ГБ RAM; Caddy — единственный фронт

Как мы это делаем

1. Ставим Caddy из официального deb-репозитория: юнит caddy.service идёт в пакете, весь конфиг — один /etc/caddy/Caddyfile
2. Ядро — три директивы: root, php_fastcgi unix//run/php/php8.3-fpm.sock, file_server; php_fastcgi сам разворачивает try_files {path} {path}/index.php index.php
3. Дожимаем: encode zstd gzip, header с HSTS/nosniff, матчер @forbidden на /wp-config.php и /xmlrpc.php → respond 403, статика с Cache-Control max-age=2592000
4. TLS не настраиваем вообще: issuers по умолчанию Let's Encrypt + резервный ZeroSSL, HTTP→HTTPS редирект с порта 80 автоматический
5. Изменения катим через caddy validate и systemctl reload caddy — graceful, без разрыва активных соединений

РЕЗУЛЬТАТ

Типовой сайт живёт на VPS за ~1000 ₽/мес вместо дорогого «битрикс-хостинга»; инциденты «забыли продлить сертификат» исчезают, а конфиг из 15–20 строк правит любой дежурный инженер.

КЛЮЧЕВОЙ НЮАНС

php_fastcgi — opinionated-шорткат: при нестандартной структуре CMS раскрываем его в expanded form и правим try_files руками; root обязан указывать на каталог с index.php.

РЕАЛИЗАЦИЯ 2 ИЗ 3

1С-Битрикс и веб-публикация 1С: остаёмся на nginx

Что настраиваем

Магазины на 1С-Битрикс и reverse-proxy перед публикацией 1С; nginx stable 1.30 + PHP-FPM 8.2

Как мы это делаем

1. Держим рекомендованную вендором связку nginx + PHP-FPM: под неё написана дока Битрикс и BitrixVM, техподдержка не разводит руками
2. TLS через certbot: systemd certbot.timer дважды в сутки, продление при остатке ≤30 дней, --deploy-hook 'systemctl reload nginx'
3. Для публикации 1С: proxy_read_timeout 300s, proxy_set_header Upgrade/Connection для WebSocket, client_max_body_size под обмены
4. Защита: limit_req_zone на /bitrix/admin/ и формы входа, ssl_protocols TLSv1.2 TLSv1.3, server_tokens off
5. Каждое изменение конфига — только через гейт nginx -t && systemctl reload nginx, правило зашито в скрипт деплоя

РЕЗУЛЬТАТ

Магазин на 18 000+ SKU с обменами 1С держит сотни запросов в секунду с запасом; остаёмся в официально поддерживаемой конфигурации Битрикс — инциденты решаем с вендором, а не вместо него.

КЛЮЧЕВОЙ НЮАНС

reload с битым конфигом nginx переживёт (останется на старом), а ребут сервера — нет: сервис не стартует. Поэтому nginx -t — не «привычка», а обязательный гейт в автоматизации.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Переезд с shared-хостинга на VPS без даунтайма

Что настраиваем

Миграции корпоративных сайтов со старых «битрикс-хостингов» на VPS под нашим обслуживанием

Как мы это делаем

1. За сутки до окна снижаем TTL A-записи до 300 с; разворачиваем полную копию сайта и БД на новом VPS
2. Проверяем копию без переключения DNS: curl --resolve site.ru:443:NEW_IP плюс hosts-файл на тестовой машине
3. Сертификат выпускаем заранее по DNS-01: в Caddy 2.11 провайдер задаётся один раз глобальной опцией dns — сайт стартует сразу с валидным TLS
4. Ночью переключаем A-запись; старый хостинг держим 5–7 дней и следим за его access-логами на остаточный трафик
5. Открываем UDP 443 в фаерволе — Caddy отдаёт HTTP/3 (включён по умолчанию с v2.6), браузеры подхватывают его через Alt-Svc

РЕЗУЛЬТАТ

Переезд проходит без даунтайма и потери позиций в поиске; клиент экономит 3000–4500 ₽/мес на хостинге, а обновление PHP перестаёт быть платной услугой хостера.

КЛЮЧЕВОЙ НЮАНС

HTTP-01 challenge не пройдёт, пока DNS смотрит на старый хостинг, — для бесшовных переездов собираем Caddy с DNS-плагином провайдера (xcaddy) и выпускаем сертификат до переключения.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Закрытый UDP 443 «выключает» HTTP/3**
  Caddy включает HTTP/3 с v2.6 по умолчанию; если фаервол пропускает только TCP, клиенты молча падают на HTTP/2. Открываем UDP 443 и проверяем Alt-Svc.

- ✕ **restart вместо reload у nginx**
  reload с ошибкой в конфиге не уронит процесс, а restart или ребут — уронит. Гейт nginx -t && reload зашиваем в скрипты, restart делаем только осознанно.

- ✕ **Rate-limit Let's Encrypt при отладке**
  Несколько неудачных валидаций в час на хост — и выпуск блокируется. Отладку ведём на staging-эндпоинте acme-staging-v02, в прод переключаемся после успеха.

- ✕ **Битрикс на Caddy «потому что модно»**
  Вендор официально поддерживает Apache/nginx. На Caddy инцидент превращается в спор с техподдержкой — для Битрикс ставим nginx + PHP-FPM без экспериментов.

- ✕ **Caddy в Docker без volume на /data**
  В /data живут ключ ACME-аккаунта и сертификаты; пересоздание контейнера без volume — перевыпуск всего и риск rate-limit. Всегда монтируем /data и /config.

- ✕ **Certbot обновил cert, nginx не узнал**
  nginx читает сертификат при старте/reload; без --deploy-hook 'systemctl reload nginx' сайт отдаёт старый cert до истечения. Хук — часть нашего шаблона.

- ✕ **Mainline nginx в проде**
  Нечётная ветка (1.31.x) первой получает новые фичи и регрессии, ngx_http_v3_module до сих пор experimental. В прод — stable 1.30.x, mainline — на стенды.

- ✕ **php_fastcgi и нестандартная CMS**
  Директива зашивает try_files {path} {path}/index.php index.php; фронт-контроллер не в корне требует expanded form с ручным rewrite.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Статика и WordPress — Caddy 2.11: Caddyfile 10–20 строк, TLS и редиректы из коробки
- Битрикс и публикация 1С — nginx stable + PHP-FPM по документации вендора
- nginx -t / caddy validate — обязательный шаг перед каждым reload

НОРМАЛЬНО

- HSTS, X-Content-Type-Options, Referrer-Policy — в шаблоне обоих серверов
- certbot.timer + deploy-hook на reload; в Caddy — контроль renewal по логам
- Мониторинг срока сертификата и HTTP-доступности с алертом в Telegram
- Кэш статики: Cache-Control public, max-age=2592000 на css/js/img/шрифты

ХОРОШО

- HTTP/3: UDP 443 открыт; для nginx — сборка с --with-http_v3_module
- DNS-01 и глобальная опция dns (Caddy 2.11) — сертификат до переключения DNS
- limit_req на логин-формы и админки + fail2ban по логам веб-сервера
- Конфиги /etc/caddy и /etc/nginx — в git, стейджинг-копия для обновлений

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Знаете ли вы, какой веб-сервер и какая ветка (stable/mainline) обслуживают ваш сайт?
- [ ] Продлевается ли SSL-сертификат автоматически и есть ли алерт за 14 дней до конца срока?
- [ ] Проверяется ли конфиг (nginx -t / caddy validate) перед каждым применением?
- [ ] Отключены ли TLS 1.0/1.1 и включён ли TLS 1.3 на боевом домене?
- [ ] Закрыты ли служебные пути: /wp-config.php, xmlrpc.php, /bitrix/admin/ с чужих IP?
- [ ] Стоит ли rate-limit на формы входа и переборные эндпоинты?
- [ ] Открыт ли UDP 443, если сайту заявлен HTTP/3?
- [ ] Лежат ли конфиги веб-сервера и сертификаты в бэкапе (а лучше — в git)?
- [ ] Поднимется ли сайт сам после внезапного ребута VPS (enabled-юниты, валидный конфиг)?
- [ ] Проверялось ли восстановление сайта из бэкапа за последний квартал?

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 VPS с Caddy или nginx под ключ: TLS, заголовки безопасности, лимиты, логи
- Переносим сайты со shared-хостинга без даунтайма: снижение TTL, DNS-01, репетиция на копии
- Настраиваем мониторинг сертификатов и доступности с алертами в Telegram
- Сопровождаем по абонентке: обновления ОС, веб-сервера и PHP, бэкапы с тестом восстановления

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 Automatic HTTPS (issuers, редиректы, renewal) (caddyserver.com — v2.11)

02 Caddyfile: директивы tls, php_fastcgi, encode, header (caddyserver.com — v2.11)

03 Модуль ngx_http_v3_module (HTTP/3, QUIC) (nginx.org — 1.31)

04 nginx: news 2026 (stable 1.30.3, mainline 1.31.2) (nginx.org — 2026)

05 Certbot User Guide (renew, deploy-hook) (eff.org — 2026)

06 Рекомендуемая среда 1С-Битрикс (nginx + PHP-FPM) (dev.1c-bitrix.ru — 2026)

07 Наш шаблон Caddyfile / nginx.conf для корпоративных сайтов (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.