



ZeroBlock

Полное руководство по настройке

RouteRich

Февраль 2026

Содержание

1. Введение	3
1.1 Что такое ZeroBlock	3
1.2 Основные возможности	3
1.3 Компоненты	4
2. Архитектура	5
2.1 Схема работы	5
2.2 Потоки данных	6
2.3 Структура файлов	6
3. Системные требования	7
3.1 Программные зависимости	7
3.2 Совместимость	7
4. Первоначальная настройка	8
5. Конфигурация через LuCI	9
5.1 Настройки (Settings)	9
5.2 Секции маршрутизации	12
5.3 Панель управления (Dashboard)	14
5.4 Диагностика	14
6. Типы секций	15
6.1 Proxy (connection_type = 'proxy')	15
6.2 VPN (connection_type = 'vpn')	15
6.3 Parental Control (Родительский контроль)	15
6.4 Параметры секций	16

7. Поддерживаемые протоколы	19
7.1 VLESS	19
7.2 VMess	19
7.3 Trojan	19
7.4 Shadowsocks	19
7.5 Hysteria2	20
7.6 SOCKS4/5	20
7.7 HTTP/HTTPS	20
7.8 Xray-core транспорты	20
8. Community Lists	21
8.1 Обзор	21
8.2 Доступные списки	21
8.3 Community Subnets (подсети)	24
8.4 Community CIDR Lists (API V2)	25
8.5 Обновление списков	26
9. DNS конфигурация	27
9.1 Архитектура DNS	27
9.2 Типы DNS	27
9.3 DNS стратегии	28
10. FakeIP	29
10.1 Принцип работы	29
10.2 Проверка FakeIP	29
10.3 Отключение FakeIP для секции	29
11. NFTables и маршрутизация	30
11.1 Структура nftables	30
11.2 Просмотр правил	30
11.3 Policy Routing	30
11.4 TPROXY	31
12. Clash API и YACD	32
12.1 Clash API	32
12.2 Использование API	32
12.3 YACD Dashboard	32
13. Устранение неполадок	33
13.1 sing-box не запускается	33
13.2 Трафик не маршрутизируется	33
13.3 Конфликт с другими сервисами	33
13.4 Высокая задержка или медленная работа	33
13.5 Opera Proху не работает	33
13.6 WARP/AmneziaWG не подключается	33
13.7 Сброс конфигурации	34



1. Введение

1.1 Что такое ZeroBlock

ZeroBlock — продвинутая система маршрутизации для OpenWrt, использующая sing-box в качестве основного движка, xray-core в качестве вспомогательного (для транспортов xhttp и mKCP) и trust tunnel. Система обеспечивает прозрачную маршрутизацию трафика на основе списков доменов и IP-адресов через прокси-серверы или VPN-интерфейсы.

Для чего это нужно: Представьте, что ваш роутер — это умный диспетчер на перекрёстке. Обычно весь ваш интернет-трафик идёт по одной дороге напрямую. ZeroBlock позволяет направлять трафик к определённым сайтам (YouTube, Telegram и др.) по альтернативным маршрутам — через прокси-серверы или VPN-туннели. При этом всё происходит прозрачно: вам не нужно ничего настраивать на телефонах, компьютерах или телевизорах — роутер сам решает, какой трафик куда отправить.

1.2 Основные возможности

Функция	Описание
Прозрачный прокси	Автоматическая маршрутизация без настройки клиентов
7+ протоколов (sing-box)	VLESS, VMess, Trojan, Shadowsocks, Hysteria2, SOCKS, HTTP
Xray-core транспорты	xhttp, mKCP (через SOCKS5-мост)
TrustTunnel	Шифрованный туннель через HTTP/2 и HTTP/3 (QUIC)
VPN интерфейсы	WireGuard, AmneziaWG, OpenVPN, GRE, L2TP, PPTP
IPv6	Прозрачное проксирование IPv6-трафика (FakeIP fc00::/18)
FakeIP DNS	Быстрое разрешение заблокированных доменов
Community Lists	YouTube, Telegram, Discord, Meta, TikTok и др.
Community CIDR Lists	IP/CIDR списки для community lists (API V2)
URLTest	Автоматический выбор лучшего прокси по задержке
Clash API	Управление и мониторинг через YACD Dashboard
Подписки	vless, clash/mihomo
Родительский контроль	Блокировка по расписанию для отдельных устройств
Автозагрузка секций	Автоматическая загрузка секций маршрутизации с сервера RouteRich (API V2)



1.3 Компоненты

Пакет	Описание
zeroblock	Основной пакет — генерация конфигурации, управление nftables
luci-app-zeroblock	Веб-интерфейс для LuCI (русская локализация встроена)

RouterRich

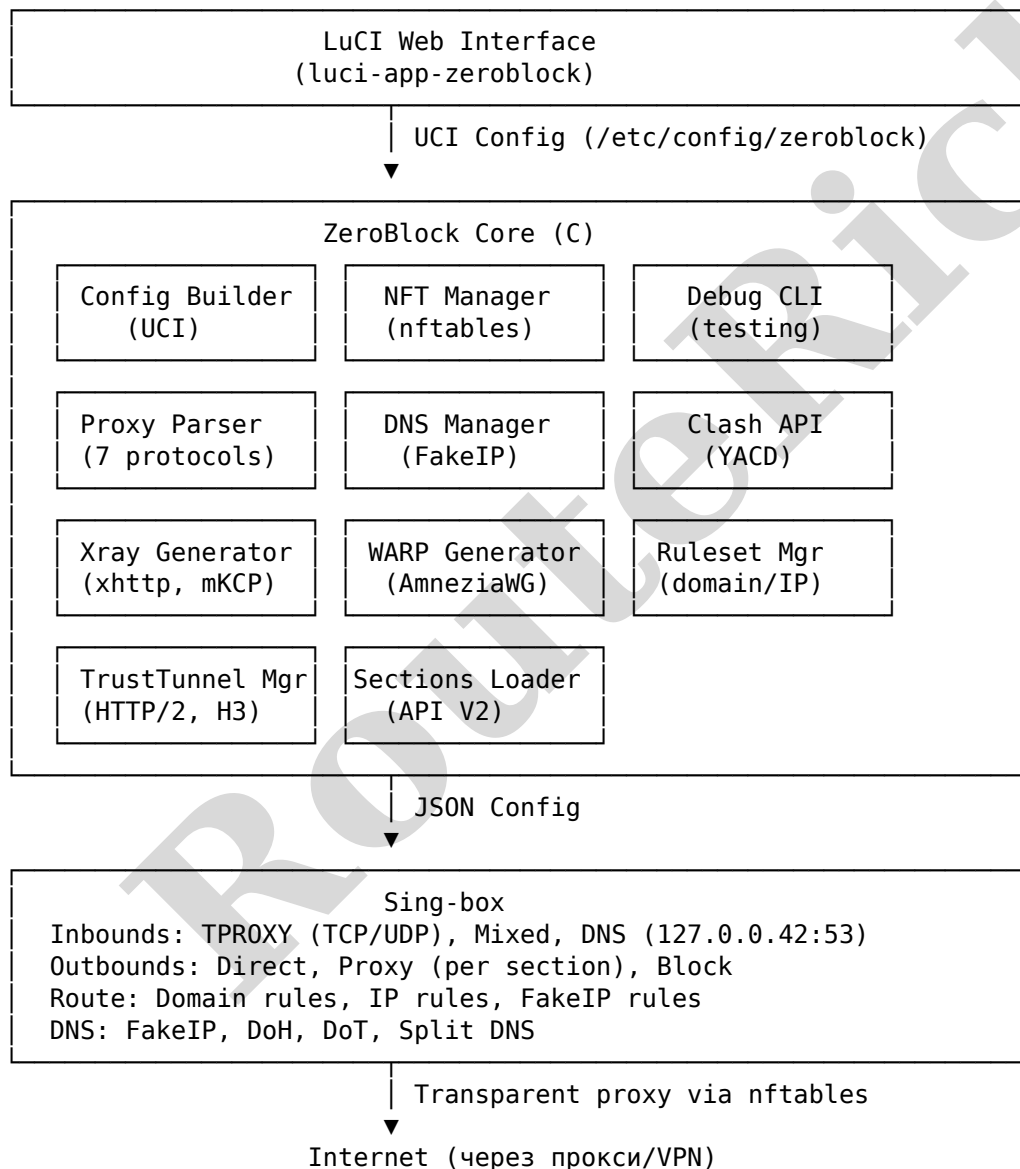


2. Архитектура

Для чего это нужно: Понимание архитектуры поможет вам быстрее находить причины проблем и эффективнее настраивать систему. Ниже показано, как компоненты ZeroBlock взаимодействуют друг с другом — от веб-интерфейса до выхода в интернет.

2.1 Схема работы

Упрощённо: вы настраиваете правила в веб-интерфейсе LuCI, ZeroBlock переводит их в конфигурацию sing-box, а sing-box и nftables обеспечивают перенаправление трафика. Вот как это выглядит в деталях:





2.2 Потоки данных

Режим FakeIP (по умолчанию):

Совет: FakeIP — это как «подменный адрес». Когда устройство в вашей сети спрашивает «где находится youtube.com?», ZeroBlock отвечает специальным ненастоящим адресом (198.18.x.x). По этому адресу роутер понимает, что трафик нужно отправить через прокси. Это быстро и надёжно.

1. **DNS-запрос клиента** -> dnsmasq -> sing-box DNS (127.0.0.42:53)
2. **Sing-box** проверяет домен по правилам:
 - Домен в списке -> возвращает FakeIP (198.18.x.x)
 - Домен не в списке -> возвращает реальный IP
3. **Трафик на FakeIP** -> перехватывается nftables -> TPROXY -> sing-box
4. **Sing-box** маршрутизирует через соответствующий outbound (прокси/VPN/direct)

Режим disable_fakeip (для отдельных секций):

Совет: Некоторые сервисы (банки, платёжные системы) проверяют, совпадает ли IP-адрес в DNS с реальным адресом сервера. Для таких случаев FakeIP нужно отключить, чтобы DNS возвращал настоящие адреса.

1. **DNS-запрос** разрешается через DNS-сервер секции -> реальный IP
2. **Трафик на реальный IP** -> маршрутизируется по IP-правилам через прокси/VPN

2.3 Структура файлов

/etc/config/zeroblock	# UCI конфигурация
/etc/init.d/zeroblock	# Init скрипт
/usr/bin/zeroblock	# CLI утилита
/tmp/zeroblock/	# Runtime директория
├─ sing-box.d/	# Sing-box конфиги
│ └─ config.json	# Основной конфиг
├─ xray.d/	# Xray-core конфиги (если используется)
│ └─ *.json	# Конфиги для xhttp/mKCP
├─ trusttunnel/	# TrustTunnel конфиги (если используется)
│ └─ *.toml	# TOML конфиги для каждой секции
├─ rulesets/	# Загруженные списки (.srs, .json)
└─ cache/	# Кэш (community lists и др.)



3. Системные требования

3.1 Программные зависимости

Устанавливаются автоматически (OpenWrt): - sing-box \geq 1.12.0 (или sing-box-tiny) - curl (для загрузки списков) - libjson-c - libuci - libubus - libpthread

Опционально, устанавливаются через автонастройку: - xray-core (для xhttp/mKCP транспортов) - trusttunnel_client (для TrustTunnel туннелей) - amneziawg-tools (для AmneziaWG/WARP) - opera-proxy (для Opera прокси) - zapret2 (для DPI bypass)

3.2 Совместимость

- **OpenWrt:** 24.10.4+
- **Архитектуры:** aarch64, x86_64

Важно: Не рекомендуется устанавливать ZeroBlock совместно с другими системами маршрутизации (mwan3, pbr), чтобы избежать конфликтов правил nftables.



4. Первоначальная настройка

После установки рекомендуется выполнить автоконфигурацию, если вы используете фирменное устройство RouteRich:

Важно: Вкладка **Автонастройка** доступна только на верифицированных устройствах RouteRich. Если ваше устройство не прошло верификацию, эта вкладка будет скрыта в интерфейсе. В таком случае все компоненты необходимо устанавливать и настраивать вручную через CLI или UCI.

1. Откройте веб-интерфейс роутера
2. Перейдите в **Службы -> ZeroBlock -> Автонастройка**
3. Включите нужные опции:
 - **Установить Opera Proxy (Install Opera Proxy)** — для секции opera
 - **Настроить AmneziaWG WARP (Configure AmneziaWG WARP)** — для секции awgl0
 - **Установить Xray (Install Xray)** — опционально, для транспортов xhttp/mKCP
 - **Установить TrustTunnel (Install TrustTunnel)** — опционально, TrustTunnel proxy
 - **Установить Zapret2 (Install Zapret2)** — опционально, для обхода DPI
 - **Автозагрузка секций (Auto-load Sections)** — автозагрузка секций маршрутизации с сервера (API V2)
 - **Автонастройка стратегий Zapret2 (Auto-configure Zapret2 strategies)** — автозагрузка новых стратегий обхода DPI
4. Нажмите **Применить**

Совет: Если вы только начинаете, включите Opera Proxy и AmneziaWG WARP — это даст вам две рабочие секции для маршрутизации без необходимости настраивать собственные прокси-серверы.



5. Конфигурация через LuCI

5.1 Настройки (Settings)

Путь: Службы -> ZeroBlock -> Настройки

5.1.1 Настройки DNS (DNS)

Для чего это нужно: DNS — это «телефонная книга» интернета, которая переводит имена сайтов (youtube.com) в числовые адреса (142.250.74.206). Настройки DNS определяют, как ZeroBlock будет выполнять эту «трансляцию» и через какие серверы.

Параметр	Описание	Значения	По умолчанию
Тип протокола DNS (DNS Protocol Type)	Протокол DNS	UDP / DoH / DoT	DoH
DNS-сервер (DNS Server)	DNS сервер	IP или URL	8.8.8.8
Bootstrap DNS (Bootstrap DNS)	Bootstrap DNS для DoH/DoT	IP	77.88.8.8
TTL	Время жизни DNS записей	Секунды	60
Стратегия (Strategy)	Стратегия разрешения имён	IPv4 Only / Prefer IPv4 / Prefer IPv6 / IPv6 Only	IPv4 Only

Совет: DoH/DoT шифрует DNS-запросы, что защищает от перехвата. Если ваш провайдер подменяет DNS-ответы, обязательно используйте DoH или DoT.

5.1.2 Сеть (Network)

Параметр	Описание
Входящие интерфейсы (Incoming Interfaces)	Интерфейсы для перехвата трафика (обычно br-lan)
Исходящий интерфейс (Custom Output)	Через какой интерфейс трафик идёт наружу (обычно не используется)
Проксировать трафик роутера (Proxy Router Traffic)	Проксировать исходящий трафик роутера, для секций с Disable FakeIP трафик проксируется всегда

Совет: WAN-интерфейсы в списке выбора помечены меткой (**wan**), чтобы было легче отличить их от локальных. Например: eth1 (ethernet) (wan).



5.1.3 Мониторинг интерфейсов (Interface Monitoring) Мониторинг VPN интерфейсов для автоматического перезапуска ZeroBlock при изменении их состояния (reconnect).

Параметр	Описание
Включить мониторинг (Enable Monitoring)	Включить мониторинг
Интерфейсы (Interfaces)	Список отслеживаемых интерфейсов (awg10 и др.)
Задержка (Delay)	Задержка перед перезагрузкой (секунды)

5.1.4 API управления (Clash API)

Параметр	Описание	По умолчанию
Включить YACD (Enable YACD)	Включить веб-dashboard для управления и мониторинга	Выкл



5.1.5 Обновление списков (List Updates)

Параметр	Описание
Интервал (Interval)	Интервал обновления списков (1d, 12h, 6h и др.)
Через секцию (Via Section)	Скачивать списки через указанную секцию
Авто двухэтапная загрузка (Auto Two-Stage Download)	Автоматически использовать двухэтапный режим при ошибке загрузки списков
Версия API (API Version)	Переключатель между V1 и V2. V2 используется по умолчанию (доступен только для устройств RouteRich)
CIDR списки сообщества (Community CIDR Lists)	Загрузка IP/CIDR списков для community lists. Можно выбрать IPv4, IPv6 или оба (только для V2)

Важно: API V2 предоставляет расширенные возможности: CIDR-списки сообщества и автозагрузку секций маршрутизации. API V2 работает только для устройств RouteRich. Если ваше устройство не поддерживается, используйте API V1(списки cidr скачиваются автоматически).

Совет: Параметр **Community CIDR Lists** (download_cidr) доступен только при выбранном API V2. Если вам нужна маршрутизация не только по доменам, но и по IP-адресам (например, для Discord Voice или Telegram), включите загрузку CIDR-списков для соответствующих семейств адресов (IPv4, IPv6 или оба).

5.1.6 Расширенные (Advanced)

Параметр	Описание	По умолчанию
Включить поддержку IPv6 (Enable IPv6 Support)	Включить FakeIP и прозрачный прокси для IPv6 (диапазон fc00::/18)	Выкл
Отключить QUIC (Disable QUIC)	Блокировать QUIC (UDP/443)	Вкл
Исключить BitTorrent (Exclude BitTorrent)	Не маршрутизировать BitTorrent	Вкл
Исключить NTP (Exclude NTP)	Не маршрутизировать NTP трафик	Вкл
Discord Voice через прокси (Discord Voice via Proxy)	Маршрутизировать голосовой трафик Discord (UDP 50000-65535) через прокси	Вкл
Уровень логирования (Log Level)	Уровень логирования	Warn
Логирование Sing-box (Sing-box logging)	Перенаправлять логи sing-box в syslog	Выкл
Логирование Xray (Xray logging)	Перенаправлять логи Xray в syslog	Выкл



Параметр	Описание	По умолчанию
Логирование TrustTunnel (TrustTunnel logging)	Перенаправлять логи TrustTunnel в syslog	Выкл
Метка Desync (Desync Mark)	Метка для zapret2 совместимости	0x40000000
Исключённые IP (Excluded IPs)	IP адреса исключённые из маршрутизации (полностью)	-

5.2 Секции маршрутизации

Путь: **Службы -> ZeroBlock -> Секции маршрутизации**

Для чего это нужно: Секции — это главный инструмент настройки ZeroBlock. Каждая секция — это правило: «трафик к таким-то сайтам отправлять через такой-то прокси/VPN». Например, можно создать секцию «youtube» с прокси-сервером и списком доменов YouTube, и весь трафик к YouTube автоматически пойдёт через прокси.

Каждая секция определяет:

- Способ подключения (прокси, VPN, блокировать/родительский контроль)
- Списки доменов/IP для маршрутизации
- Индивидуальные DNS настройки (для секций типа VPN)

Создание новой секции

1. Укажите имя секции (a-z, 0-9, подчёркивание)
2. Нажмите **Добавить**
3. Выберите тип подключения
4. Настройте прокси параметры/ выберите интерфейс VPN
5. Добавьте списки доменов или введите вручную домены/адреса в соответствующих полях (или оставьте пустым для секции catch-all)
6. Нажмите **Сохранить**
7. Нажмите **Применить**

Переименование секции Поле **Имя секции** позволяет переименовать существующую секцию. Имя может содержать латинские буквы, цифры и подчёркивание, должно начинаться с буквы. После сохранения страница перезагрузится.

Автозагрузка секций из API

Для чего это нужно: На устройствах RouteRich с API V2 секции маршрутизации могут автоматически загружаться с сервера. Это позволяет получить готовые настройки без ручной конфигурации — сервер предоставляет оптимальные секции для вашего устройства (Если вам не нужны предустановленные секции просто отключите их, если “автозагрузка секций” активна, то она будет прописывать их в конфигурацию на каждый перезапуск сервиса).

Для включения автозагрузки:

1. Убедитесь, что в настройках установлена API V2 (по умолчанию)
2. Включите опцию **Sections Auto Load** в автонастройке



При загрузке серверных секций выполняется **дедупликация** — автоматическое сравнение с пользовательскими секциями. Сравнение происходит по 7 полям:

Поле	Описание
community_lists	Списки сообщества (youtube, telegram и др.)
user_domains	Пользовательские домены (DynamicList)
user_domains_text	Пользовательские домены (текстовое поле)
user_subnets	Пользовательские подсети (DynamicList)
user_subnets_text	Пользовательские подсети (текстовое поле)
user_domain_lists	URL/пути к файлам списков доменов
user_subnet_lists	URL/пути к файлам списков подсетей

Если серверная секция содержит записи, которые уже есть в пользовательских секциях, дублирующие поля удаляются из серверной секции. Если после дедупликации серверная секция оказывается пустой (без таргетов), она автоматически отключается, чтобы не стать catch-all секцией.

Совет: Дедупликация защищает от конфликтов: если вы уже настроили секцию для YouTube, серверная секция не будет пытаться маршрутизировать тот же трафик.

Кросс-секционная валидация ZeroBlock автоматически проверяет дубликаты между секциями при генерации конфигурации. Если один и тот же домен или подсеть указан в нескольких активных секциях, в логах появится предупреждение:

```
Cross-section duplicate: domain 'example.com' in sections youtube and telegram
```

Проверяются все форматы: community_lists, user_domains (dynamic), user_domains_text, user_subnets (dynamic), user_subnets_text, а также user_domain_lists и user_subnet_lists. Отключённые секции и секции типа block не участвуют в проверке.

Важно: В веб-интерфейсе LuCI кросс-секционная валидация работает в реальном времени. Если при редактировании секции обнаружены дубликаты доменов или подсетей с другими секциями в полях DynamicList, LuCI **блокирует сохранение** и показывает предупреждение. Исправьте конфликт прежде чем сохранять.

Catch-all секция **Catch-all** — секция без списков доменов/IP. Весь трафик, не попавший в другие секции, направляется через catch-all.

Для чего это нужно: Если вы хотите, чтобы весь трафик шёл через прокси или VPN (а не только определённые сайты), создайте секцию без списков — она станет catch-all и «поймает» весь оставшийся трафик.

Особенности:

- Может быть только одна активная catch-all секция
- Если catch-all не задана, непопавший трафик идёт напрямую (direct)
- Для VPN интерфейсов рекомендуется включить **Disable FakeIP** — тогда DNS резолвится в реальные IP и маршрутизация происходит по IP-адресам через VPN туннель
- Через **Excluded Source IPs** можно исключить отдельные устройства из catch-all — их трафик будет обработан последующими секциями (по доменным спискам) или пойдёт напрямую, если не попадёт ни в одну из них
- Через **Exclusions** можно исключить отдельные домены/ip/cidr из catch-all — их трафик будет обработан последующими секциями (по доменным спискам) или пойдёт напрямую, если не попадёт ни в одну из них



Типичные сценарии:

Сценарий	Настройка catch-all
Весь трафик через прокси	Прокси-секция без списков
Весь трафик через VPN	VPN-секция без списков + Disable FakeIP
Только выбранные сайты	Не использовать catch-all

5.3 Панель управления (Dashboard)

Путь: **Службы -> ZeroBlock -> Панель управления**

Отображает:

- Информация о сервисах (sing-box, Xray, TrustTunnel, Opera Proxy, Zapret2)
- Статус всех секций с сортировкой по задержке для подписок и urltest(latency)
- Текущие задержки
- Объём трафика
- Возможность переключения прокси в селекторах
- Компактная верстка для секций с одним сервером

Автоматические функции Панели управления (Dashboard)

- **Подключение к Clash API** — автоматически при загрузке страницы
- **Тест задержки** — после первого подключения или по соответствующей кнопке
- **Сортировка по задержке** — секции автоматически сортируются
- **Мониторинг трафика** — в реальном времени через WebSocket

5.4 Диагностика

Путь: **Службы -> ZeroBlock -> Диагностика**

Выполняет автоматические проверки:

Проверка	Описание
FakeIP (роутер)	Работает ли FakeIP DNS на роутере
DNS Hijack	Перенаправлен ли DNS клиентов на sing-box
NFT правила	Загружены ли правила маршрутизации
sing-box	Запущен ли процесс sing-box
Сторонние приложения	Наличие приложений и маркировки трафика, которые могут вмешиваться в работу (zapret/zapret2 совместим)



6. Типы секций

6.1 Proxy (connection_type = 'proxy')

Маршрутизация через прокси-сервер.

Типы конфигурации прокси (proxy_config_type):

Тип	Описание
url	Прокси-ссылка (vless://, ss://, trojan://, vmess://, hysteria2://)
outbound	Полный JSON outbound конфиг sing-box
urltest	Список прокси для автоматического выбора по задержке
subscription	Base64-подписка с автоматическим обновлением
xray	Xray-core outbound JSON (для транспортов xhttp, mKCP)
trusttunnel	TrustTunnel шифрованный туннель (HTTP/2, HTTP/3)

6.2 VPN (connection_type = 'vpn')

Маршрутизация через VPN интерфейс.

Для чего это нужно: Если у вас уже настроен VPN-туннель (WireGuard, AmneziaWG, OpenVPN), ZeroBlock может направлять через него трафик к определённым сайтам. Не нужно пропускать *весь* трафик через VPN — только нужные ресурсы.

Поддерживаемые интерфейсы:

Тип	Примеры имён
WireGuard	wg0, wg1
AmneziaWG	awg0, awg10
OpenVPN	tun0, ovpn0 (не тестировалось)
GRE	gre0 (не тестировалось)
L2TP	l2tp0 (не тестировалось)
PPTP	pptp0 (не тестировалось)
Tailscale	tailscale0 (не тестировалось)

6.3 Parental Control (Родительский контроль)

Для чего это нужно: Родительский контроль позволяет ограничивать доступ в интернет для конкретных устройств (телефон ребёнка, планшет) по расписанию. Можно заблокировать как отдельные сайты (YouTube, TikTok), так и весь интернет целиком в определённые часы.

Блокировка по расписанию с фильтрацией по устройствам. Использует nftables meta hour и meta day для временных правил.

Режимы работы



Режим	Условие	Действие
Block specific	Указаны таргеты (домены/списки/IP)	Блокируются только указанные ресурсы
Block all	Таргеты не указаны	Блокируется весь интернет для устройств

Время роутера: В LuCI при настройке Parental Control отображается текущее время роутера с таймзоной. Убедитесь, что время на роутере настроено правильно (System -> System -> Time Synchronization).

Технические детали

- Поддержка перехода через полночь (22:00-07:00 -> два правила)
- Дни недели сдвигаются для второго правила при midnight crossing
- Для режима “block specific” используется dnsmasq nftset для резолва доменов
- FakeIP автоматически отключается для PC секций с таргетами

Порядок секций Порядок PC секций в LuCI имеет значение при наличии нескольких секций Parental Control:

- Правила nftables генерируются в порядке секций в конфигурации
- При пересечении source_ips между секциями сработает правило первой секции
- Порядок относительно VPN/Proxu секций не важен — PC правила всегда выполняются до маршрутизации трафика

Пример: Если устройство 192.168.1.100 указано в секциях kids_block и teens_block, и kids_block выше в списке — для этого устройства применятся правила kids_block.

6.4 Параметры секций

Общие параметры

Параметр	Описание
Включить (Enable)	Включить секцию
Тип подключения (Connection Type)	Тип: proxu, vpn, block

DNS настройки (per-section, для типа VPN)

Параметр	Описание
Тип протокола DNS (DNS Protocol Type)	udp, doh, dot
DNS-сервер (DNS Server)	DNS сервер



Параметр	Описание
Bootstrap DNS-сервер (Bootstrap DNS Server)	Bootstrap DNS для DoH/DoT
Отключить FakeIP (Disable FakeIP)	Отключить FakeIP для этой секции

Списки доменов

Параметр	Описание
Списки сообщества (Community Lists)	Community списки (youtube, telegram и др.)
Ввод пользовательских доменов (User Domains Input)	disabled, dynamic, text
Пользовательские домены (User Domains)	Пользовательские домены (dynamic)
Список пользовательских доменов (User Domains List)	Текстовый блок с доменами
Списки доменов (User Domain Lists)	URL(ссылка к списку доменов) или путь к файлу со списком доменов

Списки IP/подсетей

Параметр	Описание
Ввод пользовательских подсетей (User Subnets Input)	disabled, dynamic, text
Пользовательские подсети (User Subnets)	Пользовательские подсети (dynamic)
Список пользовательских подсетей (User Subnets List)	Текстовый блок с подсетями
Списки подсетей (User Subnet Lists)	URL(ссылка к списку IP) или путь к файлу со списком IP

Исключения (Exclusions)

Параметр	Описание
Исключения (Exclusions)	Включить исключения
Исключённые домены (Excluded Domains)	Домены исключённые из маршрутизации
Исключённые IP (Excluded IPs)	IP исключённые из маршрутизации
Исключённые из секции IP-адреса (Excluded Source IPs)	Source IP исключённые из маршрутизации

TrustTunnel параметры



Параметр	Описание
Имя хоста сервера TrustTunnel (TrustTunnel Server Hostname)	Имя хоста для TLS-соединения
Адреса серверов (Server Addresses)	Адреса сервера в формате IP:port
Имя пользователя (Username)	Имя пользователя
Пароль (Password)	Пароль
Транспортный протокол (Transport Protocol)	http2, http3
Резервный протокол (Fallback Protocol)	Резервный протокол при сбое основного
Путь к сертификату (Certificate Path)	Путь к PEM-сертификату для самоподписанных серверов
Пропустить проверку сертификата (Skip Certificate Verification)	Принимать любой сертификат
Анти-DPI (Anti-DPI)	Включить меры против DPI

URLTest параметры

Параметр	Описание
Ссылки прокси для URLTest (URLTest Proxy Links)	Список прокси-ссылок
Интервал проверки URLTest (URLTest Check Interval)	Интервал проверки (30s, 1m, 3m, 5m)
Допуск URLTest (URLTest Tolerance)	Допуск латентности в мс (50-1000)
URLTest ссылка для проверки (URLTest Testing URL)	URL для тестирования



7. Поддерживаемые протоколы

7.1 VLESS

Современный протокол с минимальным оверхедом и поддержкой Reality.

Для чего это нужно: VLESS с Reality — один из самых устойчивых к блокировкам протоколов. Он маскирует ваш трафик под обычное HTTPS-соединение с популярным сайтом, что делает его практически неотличимым от обычного веб-серфинга.

Формат URL:

```
vless://uuid@host:port?type=tcp&security=reality&pbk=key&fp=chrome  
&sni=domain&sid=id&flow=xtls-rprx-vision#Name
```

7.2 VMess

Протокол V2Ray с шифрованием.

Формат URL:

```
vmess://base64(json)
```

JSON формат:

```
{  
  "v": "2",  
  "ps": "Name",  
  "add": "server.com",  
  "port": "443",  
  "id": "uuid",  
  "aid": "0",  
  "scy": "auto",  
  "net": "ws",  
  "type": "none",  
  "host": "example.com",  
  "path": "/path",  
  "tls": "tls",  
  "sni": "example.com"  
}
```

7.3 Trojan

Протокол с маскировкой под HTTPS.

Формат URL:

```
trojan://password@host:port?sni=example.com&allowInsecure=0#Name
```

7.4 Shadowsocks

Классический протокол шифрования.

Формат URL:

```
ss://method:password@host:port#Name
```

Методы шифрования: - aes-128-gcm, aes-256-gcm - chacha20-ietf-poly1305 - 2022-blake3-aes-128-gcm, 2022-blake3-aes-256-gcm

Поддержка плагинов: да (через параметр plugin=name;opts в URL)



7.5 Hysteria2

Высокопроизводительный протокол на базе QUIC.

Совет: Hysteria2 особенно хорошо работает в сетях с высокой потерей пакетов (мобильный интернет, нестабильный Wi-Fi), так как QUIC имеет встроенную коррекцию ошибок.

Формат URL:

hysteria2://password@host:port?sni=example.com&insecure=0#Name

7.6 SOCKS4/5

Классический SOCKS прокси.

Формат URL:

socks5://user:password@host:port#Name

socks4://host:port#Name

7.7 HTTP/HTTPS

HTTP прокси с опциональной авторизацией.

Формат URL:

http://user:password@host:port#Name

https://user:password@host:port#Name

7.8 Xray-core транспорты

VLESS/VMess с транспортом xhttp и mKCP маршрутизируются через xray-core с SOCKS5-мостом.

xhttp транспорт:

vless://uuid@host:port?type=xhttp&path=/path&security=tls#Name

mKCP транспорт:

vless://uuid@host:port?type=kcp&seed=seed&headerType=wireguard#Name



8. Community Lists

8.1 Обзор

Community Lists — встроенные списки доменов для популярных сервисов. Списки загружаются из репозитория `itdoginfo/allow-domains`.

Для чего это нужно: Вместо того чтобы вручную добавлять десятки доменов YouTube или Telegram, достаточно выбрать соответствующий community list. Списки поддерживаются сообществом и регулярно обновляются.

8.2 Доступные списки

Формат списков зависит от версии API:

- **API V1** — списки загружаются в формате `.srs` (sing-box rule-set) из GitHub Releases. Подсети загружаются отдельно в формате `.lst`.
- **API V2** — списки загружаются с сервера RouteRich в формате JSON (`_domains.json`, `_ipv4.json`, `_ipv6.json`). Домены и CIDR-подсети объединены в одном источнике. Доступно только для устройств RouteRich. При ошибке авторизации происходит автоматический fallback на V1.

Списки API V1 Доступны для всех устройств. Загружаются в формате `.srs` из GitHub.

Список	Описание
block	Заблокированные ресурсы
geoblock	Сайты с геоблокировкой
discord	Discord (голос, видео, CDN)
meta	Facebook, Instagram, WhatsApp
telegram	Telegram мессенджер
tiktok	TikTok
twitter	Twitter/X
youtube	YouTube видеоплатформа
hdrezka	HDRezka онлайн-кинотеатр
anime	Аниме стриминговые сайты
news	Новостные сайты
porn	Взрослый контент
hodca	HODCA сервисы
google_ai	Google AI (Gemini)
google_play	Google Play Store
cloudflare	Cloudflare CDN и сервисы
cloudfront	AWS CloudFront CDN
digitalocean	DigitalOcean хостинг
hetzner	Hetzner хостинг
ovh	OVH хостинг
roblox	Roblox игровая платформа
russia_inside	Сайты заблокированные в РФ
russia_outside	Российские сайты недоступные за рубежом



Список	Описание
ukraine_inside	Сайты заблокированные в Украине

Списки API V2 Доступны только для устройств RouteRich. Загружаются в формате JSON с сервера. Включают расширенный набор списков с CIDR-подсетями.

Блокировки и гео-ограничения

Список	Описание
block	Заблокированные ресурсы РКН
geoblock	Геоблокировки, JetBrains

Социальные сети и мессенджеры

Список	Описание
discord	Discord (голос, видео, CDN)
meta	Facebook, Instagram, WhatsApp, Messenger
messengers	Telegram, Signal, Viber, Zello
socials	TikTok, X/Twitter, LinkedIn, Patreon, Snapchat

Видео и стриминг

Список	Описание
youtube	YouTube видеоплатформа
video	HDRezka, Netflix, KinoPub, Filmix, LostFilm, дорамы
anime	Crunchyroll, Anilibria, JUT.SU, Shikimori, манга

Музыка

Список	Описание
music	Spotify, Deezer, Tidal, SoundCloud, MusicBrainz

Новости

Список	Описание
news	Meduza, BBC, DW, Дождь, независимые СМИ

AI сервисы



Список	Описание
ai	ChatGPT, Claude, Gemini, Grok, Copilot, Canva

Google

Список	Описание
googleplay	Google Play Store

Игры

Список	Описание
games	Roblox, Chess.com, EVE Online, Itch.io, Modrinth

Магазины

Список	Описание
shop	Zara, Massimo Dutti, COS, H&M Group

Инструменты

Список	Описание
tools	Proton Mail, Medium, FastPic, VPN-сервисы

Репозитории

Список	Описание
repo	Docker Hub, GitHub Packages, NPM, PyPI

Торренты

Список	Описание
torrent	RuTracker, RuTor, Kinozal, NNM-Club, 1337x

Взрослый контент

Список	Описание
porn	PornHub, XVideos, RedTube



Искусство

Список	Описание
art	DeviantArt

CDN и облачные провайдеры

Список	Описание
cdn_akamai	Akamai CDN, edge services
cdn_aws	Amazon Web Services, CloudFront
cdn_azure	Microsoft Azure cloud
cdn_bunny	Bunny.net CDN
cdn_cdn77	CDN77 content delivery
cdn_cloudflare	Cloudflare CDN, DDoS protection, DNS
cdn_digitalocean	DigitalOcean cloud
cdn_fastly	Fastly CDN, edge cloud
cdn_gcore	Gcore CDN, edge network
cdn_github	GitHub Pages, API, Actions, Packages
cdn_google	Google Cloud, 1e100.net, gstatic
cdn_hetzner	Hetzner Online, Hetzner Cloud
cdn_linode	Linode (Akamai Connected Cloud)
cdn_oracle	Oracle Cloud Infrastructure
cdn_ovh	OVHcloud hosting
cdn_scaleway	Scaleway cloud hosting
cdn_selectel	Selectel хостинг
cdn_vultr	Vultr cloud hosting
cdn_yandex	Яндекс, Яндекс.Облако

8.3 Community Subnets (подсети)

Помимо доменных списков (.srs), для некоторых сервисов доступны списки IP-подсетей (.lst). Подсети загружаются из [itdoginfo/allow-domains/Subnets](https://itdoginfo.com/allow-domains/Subnets) и добавляются в nftables sets для маршрутизации по IP-адресам.

Для чего это нужно: Некоторые сервисы (Discord Voice, Telegram) используют прямые IP-подключения, минуя DNS. В этом случае доменные списки не помогут — нужны списки IP-адресов. Community Subnets решают эту задачу.

Доступные списки подсетей (IPv4 и IPv6):

Список	Описание
discord	Discord серверы (голос, медиа, API)
meta	Meta серверы (Facebook, Instagram, WhatsApp)
telegram	Telegram серверы



Список	Описание
twitter	Twitter/X серверы
cloudflare	Cloudflare CDN
cloudfront	Amazon CloudFront CDN
digitalocean	DigitalOcean
hetzner	Hetzner хостинг
ovh	OVH хостинг
roblox	Roblox игровые серверы

Подсети загружаются автоматически при наличии соответствующего списка в `community_lists` секции. Если `.lst` файл не существует для данного списка (например, `youtube`), это не является ошибкой — для таких сервисов работает только доменная маршрутизация.

8.4 Community CIDR Lists (API V2)

Важно: Функция доступна только при использовании API V2 на устройствах RouteRich.

При включённом API V2 в разделе **Обновление списков** доступен параметр **Community CIDR Lists** (`download_cidr`). Он позволяет загружать IP/CIDR списки для community lists с сервера. Можно выбрать:

- **IPv4** — загрузка только IPv4 CIDR-списков
- **IPv6** — загрузка только IPv6 CIDR-списков
- **Оба** — загрузка IPv4 и IPv6

CIDR-списки дополняют доменные списки, обеспечивая маршрутизацию трафика, который идёт напрямую по IP-адресам. API V2 предоставляет агрегированные CIDR-диапазоны (отдельные IP автоматически объединяются в подсети /24 для IPv4)(Используйте, если вам это необходимо).

Discord Voice Опция **Discord Voice via Proxy** (`discord_voice`) управляет маршрутизацией голосового UDP трафика Discord (порты 50000-65535) через прокси:

- **Включено** (по умолчанию): весь UDP трафик выбранных списков идёт через прокси
- **Выключено:** UDP порты 50000-65535 исключены из маршрутизации для Discord — голосовой трафик идёт напрямую или через `zapret/zapret2`

UDP правила для community subnets создаются только для протоколов, поддерживающих UDP:

Тип соединения	TCP	UDP
VLESS, VMess, Trojan, Shadowsocks, Hysteria2	да	да
SOCKS5	да	да
HTTP/HTTPS	да	нет
SOCKS4	да	нет
VPN (AmneziaWG, WireGuard)	да	да



8.5 Обновление списков

Ручное обновление

zeroblock update_lists

Автоматическое обновление настраивается в LuCI

Settings -> List Updates -> Interval

RouterRich

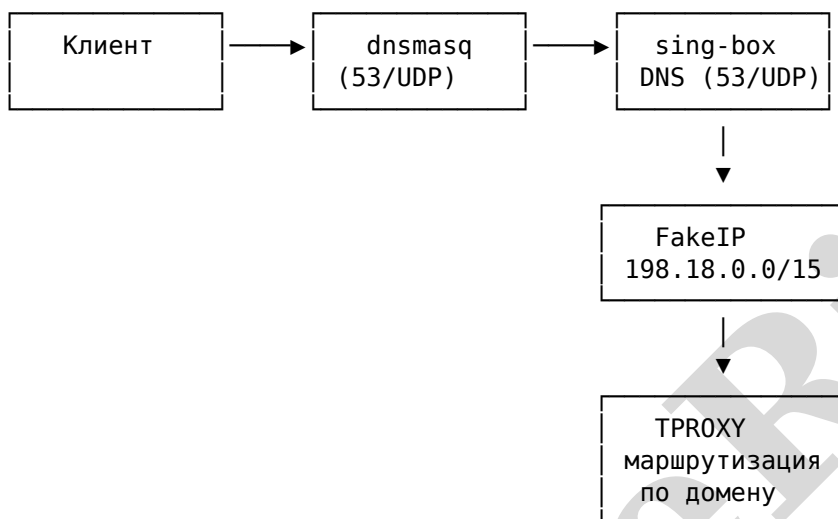


9. DNS конфигурация

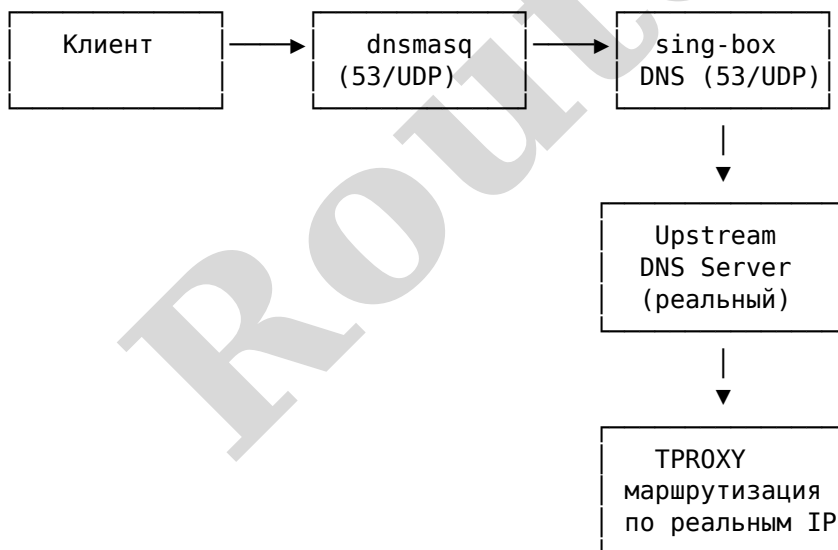
9.1 Архитектура DNS

Для чего это нужно: Понимание работы DNS в ZeroBlock поможет диагностировать проблемы. Ключевая идея: ZeroBlock «перехватывает» DNS-запросы и для заблокированных доменов возвращает специальные FakeIP-адреса, по которым трафик автоматически направляется через прокси.

Стандартный режим (FakeIP):



Режим disable_fakeip (реальные IP):



Режим disable_fakeip используется для сервисов, которые проверяют соответствие IP.

9.2 Типы DNS

Тип	Описание	Пример
UDP	Стандартный DNS	8.8.8.8



Тип	Описание	Пример
DoH	DNS over HTTPS	https://dns.google/dns-query
DoT	DNS over TLS	tls://dns.google

9.3 DNS стратегии

Стратегия	Описание
ipv4_only	Только IPv4 адреса
prefer_ipv4	Предпочитать IPv4
prefer_ipv6	Предпочитать IPv6
ipv6_only	Только IPv6 адреса



10. FakeIP

10.1 Принцип работы

Для чего это нужно: FakeIP — ключевая технология sing-box. Представьте себе почтовую службу: когда вы отправляете письмо на «виртуальный адрес» (FakeIP), почтальон (sing-box) знает, что это письмо нужно переслать через специальный канал (прокси). Это позволяет быстро и без утечек маршрутизировать трафик.

FakeIP — технология, при которой sing-box возвращает виртуальные IP-адреса из специального диапазона для доменов в списках маршрутизации. Это позволяет:

1. Быстро определять, нужно ли маршрутизировать трафик
2. Избегать DNS-утечек
3. Ускорить первое подключение к сайту

Диапазон FakeIP IPv4: 198.18.0.0/15 (198.18.0.0 - 198.19.255.255)

Диапазон FakeIP IPv6: fc00::/18 (при включённой поддержке IPv6)

10.2 Проверка FakeIP

```
# Домен в списке -> FakeIP
nslookup youtube.com 127.0.0.42
# Server:      127.0.0.42
# Address:     127.0.0.42#53
# Name:        youtube.com
# Address:     198.18.0.1
```

```
# Домен не в списке -> реальный IP
nslookup example.com 127.0.0.42
# Server:      127.0.0.42
# Address:     127.0.0.42#53
# Name:        example.com
# Address:     93.184.216.34
```

10.3 Отключение FakeIP для секции

Для некоторых сервисов (например, Cloudflare) может потребоваться отключение FakeIP:

```
uci set zeroblock.cloudflare.disable_fakeip='1'
uci commit zeroblock
/etc/init.d/zeroblock restart
```



11. NFTables и маршрутизация

11.1 Структура nftables

Для чего это нужно: nftables — это встроенный в Linux межсетевой экран. ZeroBlock использует его как «диспетчера трафика»: nftables решает, какие пакеты отправить в sing-box для проксирования, а какие пропустить напрямую. Понимание структуры nftables полезно для отладки.

ZeroBlock создаёт таблицу `inet zeroblock` со следующими цепочками:

```
table inet zeroblock {
    chain prerouting {
        type filter hook prerouting priority mangle; policy accept;
        # Перенаправление DNS на sing-box
        # Перенаправление трафика через TPROXY
    }

    chain output {
        type route hook output priority mangle; policy accept;
        # Маршрутизация трафика роутера (опционально)
    }

    set bypass_ips { ... } # IP для прямого доступа
    set routed_ips { ... } # IP для маршрутизации
}
```

11.2 Просмотр правил

Все правила

```
nft list table inet zeroblock
```

Количество цепочек

```
nft list chains inet zeroblock | wc -l
```

Содержимое set

```
nft list set inet zeroblock bypass_ips
```

11.3 Policy Routing

ZeroBlock настраивает policy routing для направления помеченных пакетов:

Просмотр правил

```
ip rule show
```

Правило для zeroblock

```
# 100:    from all fwmark 0x1 lookup 100
```

Таблица маршрутизации

```
ip route show table 100
```



11.4 TPROXY

Для чего это нужно: TPROXY (Transparent Proxy) — это механизм ядра Linux, который позволяет перенаправлять сетевые пакеты в sing-box без изменения их заголовков. Благодаря этому устройства в сети не знают о существовании прокси — для них всё выглядит как обычное интернет-соединение.

Для прозрачного проксирования используется TPROXY (transparent proxy):

- **Порт TPROXY:** 2154 (фиксированный)
 - **Метка пакетов:** 1 (фиксированная)
-

RouterRich



12. Clash API и YACD

12.1 Clash API

Clash API позволяет:

- Получать список прокси и их статус
- Тестировать задержку
- Переключать активный прокси в селекторах
- Мониторить трафик в реальном времени

Endpoints:

Endpoint	Метод	Описание
/proxies	GET	Список всех прокси
/proxies/{name}	GET	Информация о прокси
/proxies/{name}/delay	GET	Тест задержки
/group/{name}	PUT	Переключить прокси в группе
/traffic	WS	Поток данных о трафике
/logs	WS	Поток логов

12.2 Использование API

Получить список прокси

```
curl http://127.0.0.1:9090/proxies
```

Тест задержки

```
curl "http://127.0.0.1:9090/proxies/youtube/delay?\nurl=http://www.gstatic.com/generate_204&timeout=5000"
```

Переключить прокси в группе

```
curl -X PUT http://127.0.0.1:9090/group/youtube -d '{"name": "proxy1"}
```

12.3 YACD Dashboard

YACD — веб-интерфейс для управления sing-box через Clash API.

Доступ: `http://<router-ip>:9090/ui`

Функции:

- Просмотр всех прокси и групп
- Тестирование задержки
- Переключение активного прокси
- Мониторинг трафика в реальном времени
- Просмотр логов



13. Устранение неполадок

13.1 sing-box не запускается

Симптомы: Сервис не стартует, прокси не работает

Сначала включите логи:

1. Настройки > Уровень логирования = debug
2. Настройки > Логирование sing-box = 1
3. Нажмите **Применить**

Диагностика: Вкладка **Диагностика** — соответствующие кнопки для просмотра логов и конфигурации.

Решения:

1. Проверьте правильность прокси-ссылок
2. Убедитесь, что sing-box-tiny установлен

13.2 Трафик не маршрутизируется

Симптомы: Сайты не открываются через прокси, FakeIP не работает

Диагностика: Настройки > Включить YACD > Нажать **Применить** > Нажать **Открыть YACD**

Решения:

1. Убедитесь, что секция включена (enabled='1')
2. Проверьте, что домен есть в списках
3. Перезапустите сервис через Панель управления

13.3 Конфликт с другими сервисами

Симптомы: Конфликты с mwan3, rbr, или другими системами маршрутизации

Решения:

1. Отключите конфликтующие сервисы
2. Используйте разные метки (marks) для разных систем
3. Проверьте порядок правил nftables

13.4 Высокая задержка или медленная работа

Диагностика: Панель управления > Тестирование задержки

Решения:

1. Используйте URLTest для автовыбора лучшего прокси
2. Выберите сервер ближе географически

13.5 Opera Проху не работает

Решения: Система > Автозапуск > opera-proxu > перезапустить

13.6 WARP/AmneziaWG не подключается

Диагностика:

```
# Пинг через интерфейс  
ping -I awg10 8.8.8.8
```



Решения:

Переконфигурировать WARP (только для фирменных устройств RouteRich)
zeroblock awg warp

Проверить internet-detector (только для фирменных устройств RouteRich)
zeroblock awg internet_detector

13.7 Сброс конфигурации

Остановить сервис
/etc/init.d/zeroblock stop

Удалить конфигурацию
rm -f /etc/config/zeroblock

Удалить и заново установить пакеты

Документ создан: Февраль 2026 Версия ZeroBlock: 0.6.4(Beta)