



ПОЛНАЯ ИНСТРУКЦИЯ · ВЕРСИЯ 3 · 20 ОКТЯБРЯ 2026

Роутер с VPN для всего офиса

GL.iNet GL-MT3000 (Beryl AX) и miHoMo: один раз настроили — все устройства в сети ходят через ваш VPN-сервер, а банки, маркетплейсы и телефония — напрямую.

8 шагов

от коробки до работы

~2 часа

с первого раза

2 VPN

свой сервер и узел для видео

OpenWrt 21.02

прошивка GL 4.8.1

miHoMo 1.19

движок Clash Verge

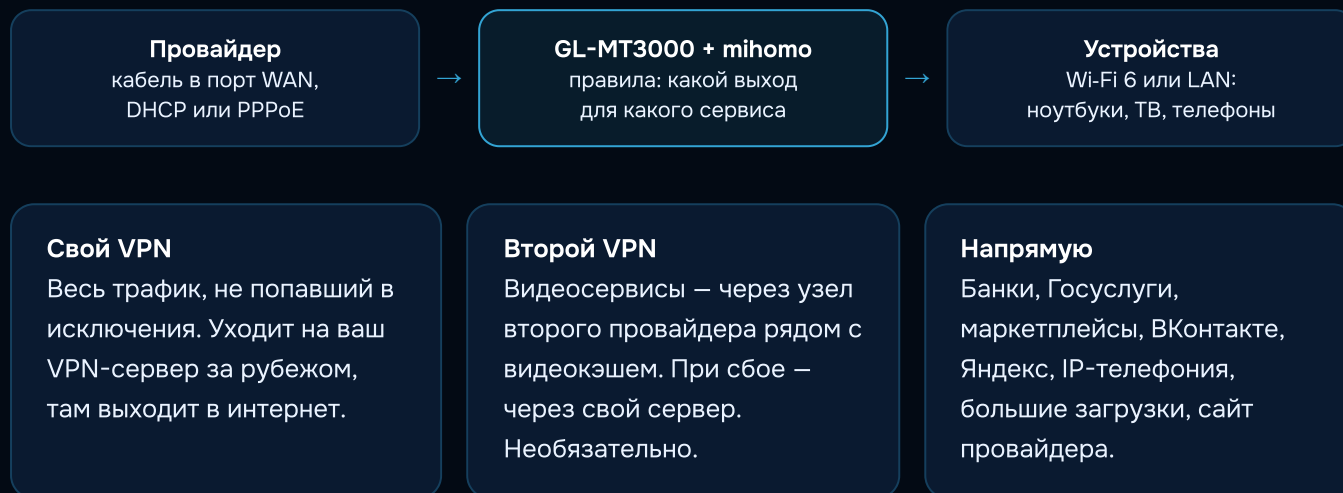
СОДЕРЖАНИЕ

- | | | | |
|--------------------|-------------------------------------|--------------------|---|
| 01 | Что получится и что понадобится | 08 | Шаг 7. Брандмауэр и DNS |
| 02 | Шаг 1. Первое включение и пароль | 09 | Шаг 8. Проверка |
| 03 | Шаг 2. Подключение к провайдеру | 10 | Два VPN: отдельный узел для видео |
| 04 | Шаг 3. LuCI, SSH-ключ, точное время | 11 | Исключения, большие загрузки, телевизор |
| 05 | Шаг 4. Установка miHoMo | 12 | Обслуживание и безопасность |
| 06 | Шаг 5. Конфиг miHoMo | 13 | Габри и диагностика · чек-лист |
| 07 | Шаг 6. Служба и автозапуск | | |

01

Что получится и что понадобится

Роутер становится единственной точкой, где живёт VPN. На устройствах ничего не ставится и не настраивается.



Как устроено внутри

- **TUN-интерфейс** **Meta** забирает трафик самого роутера и всех устройств локальной сети.
- **DNS в режиме fake-ip**. Устройства спрашивают DNS у роутера (dnsmasq), он передаёт запрос в mihomo. Так mihomo узнаёт имя сайта и применяет правило.
- **Sniffer** определяет сайт по самому соединению (TLS, HTTP, QUIC). Исключения работают даже у устройств со своим DNS, например у браузера с DNS-over-HTTPS.
- **Отдельная группа для видео** с узлом второго VPN-провайдера и запасным выходом через свой сервер (раздел 10).
- **Группа серверов в режиме fallback**. Работает первый живой сервер по порядку, проверка раз в 5 минут, при сбое — автоматическое переключение на следующий.
- **Служебное правило маршрутизации 5990** не даёт фирменной прошивке GL.iNet увести трафик локальной сети мимо VPN (подробно — в шаге 6).

Что понадобится

ЧТО	ТРЕБОВАНИЯ	ЗАЧЕМ
Роутер	GL.iNet GL-MT3000 (Beryl AX) или любой с OpenWrt, от 256 МБ ОЗУ и 128 МБ флеш-памяти	mihomo весит около 35 МБ и держит правила в памяти
VPN-сервер	Свой сервер с панелью x-ui / 3x-ui или Xray, минимум два протокола: VLESS + Reality и VLESS + WebSocket + TLS	Резерв на случай, если один протокол не пройдёт
Профиль клиента	Рабочий профиль Clash Verge / mihomo (раздел proxies) или данные подключения из панели	Серверы переносятся в конфиг роутера
Данные провайдера	Тип подключения: DHCP или PPPoE; для PPPoE — логин и пароль из договора	Без них роутер не выйдет в интернет

Компьютер	Windows, macOS или Linux с терминалом и OpenSSH; патч-корд	Настройка по SSH
Список сервисов	Банки, CRM, телефония, маркетплейсы, которыми вы пользуетесь	Это ваши исключения

Про «китайскую версию». На маркетплейсах роутер часто продают с пометкой «Китайская версия» — это прошивка с регионом CN. В части старых CN-прошивок вырезали VPN-функции, но для этой схемы они не нужны: клиент ставится свой. Проверьте сразу после покупки, что прошивка 4.x или новее и что в «Расширенных настройках» есть установка LuCI. Если нет — роутер прошивается на международную версию через аварийный загрузчик (U-Boot).

02 · ШАГ 1

Первое включение и пароль

Пока роутер не подключён к провайдеру, работаем с ним по кабелю.

1. Подключите питание USB-C (адаптер 5 В / 3 А) и соедините компьютер с портом **LAN** патч-кордом.
2. Откройте в браузере `http://192.168.8.1`, выберите язык и задайте **пароль администратора**. Он же будет паролем пользователя `root` для LuCI и SSH.
3. В разделе **Wireless** смените имена сетей и **заводской пароль Wi-Fi** с наклейки. Это частая забытая мелочь.
4. В **System** → **Upgrade** посмотрите версию прошивки. Нужна 4.x и новее; эта инструкция проверена на 4.8.1.

Компьютер подключён к двум сетям? Если он одновременно в другой сети по Wi-Fi, Windows может решить, что кабель к роутеру главнее, и пустить туда весь интернет. Пока у роутера нет своего интернета, связь пропадёт. Задайте кабельному адаптеру ручную метрику 500 — тогда по кабелю компьютер будет ходить только к роутеру:

```
# PowerShell от имени администратора
Set-NetIPInterface -InterfaceAlias "Ethernet" -InterfaceMetric 500
# вернуть как было:
Set-NetIPInterface -InterfaceAlias "Ethernet" -AutomaticMetric Enabled
```

03 · ШАГ 2

Подключение к провайдеру

Кабель провайдера (или от оптического терминала) — в порт WAN 2,5 Гбит/с.

Откройте **Internet** в панели GL.iNet. Если роутер долго висит в состоянии **Connecting...**, провайдер подключает не по DHCP, а по **PPPoE**. Выберите PPPoE и введите логин и пароль из договора или личного кабинета. То же самое из терминала:

```
# PPPoE (логин и пароль из договора)
uci set network.wan.proto='pppoe'
uci set network.wan.username='LOGIN'
uci set network.wan.password='PASSWORD'
```

```
uci commit network
ifup wan

# проверка: адрес на WAN и выход в интернет
ifstatus wan | grep -A2 ipv4-address
ping -c 3 77.88.8.8
```

Адрес вида 100.64.x.x – 100.127.x.x на WAN – это CGNAT провайдера, для схемы он не мешает: роутер сам открывает соединение к VPN-серверу, входящие подключения не нужны.

04 • ШАГ 3

LuCI, SSH-ключ и точное время

Дальше всё делается из терминала по SSH-ключу, без паролей.

3.1 Установите LuCI

В панели GL.iNet: **System** → **Advanced Settings** → **Install LuCI**. После установки она открывается по адресу `http://192.168.8.1/cgi-bin/luci` с логином `root`.

LuCI на прошивке GL работает частично. Её служебный адрес `/ubus` перехватывает панель GL.iNet, поэтому часть форм, например добавление SSH-ключей, не сохраняется. Смотреть настройки в LuCI удобно, а менять – надёжнее через SSH.

3.2 Добавьте SSH-ключ

Если ключа ещё нет, создайте его: `ssh-keygen -t ed25519`. Затем добавьте публичную часть на роутер (один раз введите пароль администратора):

```
# Windows PowerShell
type $env:USERPROFILE\.ssh\id_ed25519.pub | ssh root@192.168.8.1 "cat >> /etc/dropbear/authorized_keys"

# macOS / Linux
cat ~/.ssh/id_ed25519.pub | ssh root@192.168.8.1 "cat >> /etc/dropbear/authorized_keys"

# проверка: вход без пароля
ssh root@192.168.8.1 "uname -m; cat /etc/glversion" # aarch64 и версия прошивки
```

3.3 Синхронизируйте время

После включения роутер может не знать точного времени, пока у него не появится интернет. С неверной датой не проверяются TLS-сертификаты, и VPN не поднимется.

```
date
ntpd -q -p 0.openwrt.pool.ntp.org
date
```

3.4 Проверьте пакеты

Для TUN нужны модуль ядра и полная версия `ip`. На прошивке GL 4.x они обычно уже стоят:

```
opkg list-installed | grep -E "(kmod-tun|ip-full|curl|ca-bundle) "  
# если чего-то нет:  
opkg update && opkg install kmod-tun ip-full curl ca-bundle
```

05 · ШАГ 4

Установка mihomo

mihomo — тот же движок, что внутри Clash Verge. Поддерживает VLESS, Reality, WebSocket, Hysteria2 и десяток других протоколов.

Роутер может не достигаться до GitHub напрямую, поэтому файл удобнее скачать на компьютер и передать по SSH. Для GL-MT3000 нужна сборка **linux-arm64**. Актуальная версия — на странице релизов github.com/MetaCubeX/mihomo/releases; ниже — версия, на которой проверена инструкция.

```
# 1. На компьютере: скачать и передать на роутер  
curl -LO https://github.com/MetaCubeX/mihomo/releases/download/v1.19.32/mihomo-linux-arm64-v1.19.32.gz  
scp -O mihomo-linux-arm64-v1.19.32.gz root@192.168.8.1:/tmp/mihomo.gz  
# ключ -O нужен: на роутере dropbear без SFTP  
  
# 2. На роутере: распаковать и проверить  
ssh root@192.168.8.1  
gunzip -c /tmp/mihomo.gz > /usr/bin/mihomo && rm /tmp/mihomo.gz  
chmod +x /usr/bin/mihomo  
mihomo -v # Mihomo Meta v1.19.32 linux arm64  
mkdir -p /etc/mihomo  
df -h /overlay # свободного места должно остаться с запасом
```

Файлы GeoIP не нужны. В этой схеме нет правил GEOIP и GEOSITE: исключения заданы доменами и подсетями. Поэтому mihomo не будет скачивать базы при старте, а флеш-память не расходуется.

06 · ШАГ 5

Конфиг mihomo

Файл `/etc/mihomo/config.yaml`. Ниже — рабочий конфиг с роутера; ключи, адреса и домены заменены на заглушки.

ЗАГЛУШКА	ЧТО ПОДСТАВИТЬ	ГДЕ ВЗЯТЬ
<code>SERVER_IP</code>	IP-адрес VPN-сервера	панель хостинга
<code>PORT_1</code> , <code>PORT_2</code>	порты входов Reality на сервере	настройки входов в x-ui
<code>vpn.example.ru</code>	свой домен, указывающий на сервер	DNS вашего домена
<code>UUID</code> , <code>PUBLIC_KEY</code> , <code>SHORT_ID</code>	данные клиента и входа Reality	панель x-ui или профиль Clash Verge
<code>/ws-path</code>	путь WebSocket-входа	настройки входа в x-ui
<code>SECRET</code>	пароль панели управления mihomo	придумайте: <code>head -c 24 /dev/urandom base64</code>

<code>provider.ru</code>	сайт вашего провайдера	чтобы личный кабинет открывался напрямую
<code>VIDEO_NODE</code> , <code>UUID_2</code> , <code>SNI_2</code>	узел второго VPN-провайдера для видео (необязательно)	подписка второго провайдера в Clash Verge, раздел 10
<code>video.example</code>	домены видеосервиса и его CDN	список соединений mihome, раздел 11
<code>TV_MAC</code>	MAC-адрес телевизора	список клиентов в панели GL.iNet

Самый быстрый путь — открыть в Clash Verge на компьютере **Профили** → **Редактировать файл** и скопировать оттуда раздел `proxies` целиком: серверы перенесутся без правок. Затем у каждого сервера поменяйте `client-fingerprint` на `safari` (почему — в разделе «Габбли»).

```
/ETC/MINOMO/CONFIG.YAML · ЧАСТЬ 1: ОСНОВА, TUN, DNS, SNIFFER
```

```
mode: rule
log-level: warning
ipv6: false
allow-lan: false
unified-delay: true
tcp-concurrent: true
find-process-mode: 'off'
external-controller: 192.168.8.1:9090    # панель управления и API
secret: SECRET
profile:
  store-selected: true

tun:
  enable: true
  stack: mixed
  device: Meta                        # имя интерфейса, на него ссылается брандмауэр
  auto-route: true
  auto-detect-interface: true
  strict-route: false
  mtu: 1500
  dns-hijack:
    - any:53
  route-exclude-address:              # это не заворачивать в туннель
    - 10.0.0.0/8
    - 100.64.0.0/10
    - 172.16.0.0/12
    - 192.168.0.0/16
    - SERVER_IP/32                    # сам VPN-сервер – иначе петля

dns:
  enable: true
  listen: 127.0.0.1:1053                # сюда dnsmasq отправит запросы (шаг 7)
  ipv6: false
  enhanced-mode: fake-ip
  fake-ip-range: 198.18.0.1/16
  fake-ip-filter:                      # этим доменам – настоящие адреса
    - '*.lan'
    - '*.local'
    - '*.arpa'
    - time.*.com
    - ntp.*.com
    - '*.msftncsi.com'
    - www.msftconnecttest.com
    - +.pool.ntp.org
    - +.gl-inet.com
    - +.provider.ru
    - +.vk.ru
    - +.vk.com
    - +.userapi.com
    - +.vkuser.net
    - +.mycdn.me
    - +.mail.ru
    - +.rustore.ru
    - +.max.ru
    - +.avito.ru
    - +.avito.st
    - +.2gis.ru
    - +.2gis.com
  default-nameserver:
    - 77.88.8.8
    - 8.8.8.8
  nameserver:
    - https://dns.google/dns-query
```

```
- https://cloudflare-dns.com/dns-query
proxy-server-nameserver:      # чтобы найти адрес VPN-сервера
- 77.88.8.8
- https://dns.google/dns-query
direct-nameserver:           # для исключений — российский DNS
- 77.88.8.8
- 77.88.8.1
```

```
sniffer:
  enable: true
  force-dns-mapping: true
  parse-pure-ip: true
  override-destination: false
  sniff:
    HTTP: { ports: [80, 8080-8880] }
    TLS: { ports: [443, 8443] }
    QUIC: { ports: [443, 8443] }
```

ЧАСТЬ 2: СЕРВЕРЫ — ОТ ОСНОВНОГО К ЗАПАСНЫМ

```
proxies:
# 1. Основной: VLESS + Reality, маскируется под ваш собственный домен на этом же сервере
- name: "Reality (свой домен)"
  type: vless
  server: SERVER_IP
  port: PORT_1
  uuid: UUID
  network: tcp
  tls: true
  udp: true
  flow: xtls-rprx-vision
  servername: vpn.example.ru
  reality-opts:
    public-key: PUBLIC_KEY
    short-id: SHORT_ID
  client-fingerprint: safari

# 2. Резервный Reality на другом порту (свой SNI)
- name: "Reality (резерв)"
  type: vless
  server: SERVER_IP
  port: PORT_2
  uuid: UUID
  network: tcp
  tls: true
  udp: true
  flow: xtls-rprx-vision
  servername: sni.example.com
  reality-opts:
    public-key: PUBLIC_KEY
    short-id: SHORT_ID
  client-fingerprint: safari

# 3. VLESS + WebSocket через TLS на 443 (сертификат на ваш домен)
- name: "WebSocket TLS"
  type: vless
  server: vpn.example.ru
  port: 443
  uuid: UUID
  network: ws
  tls: true
  udp: true
  servername: vpn.example.ru
```

```

ws-opts:
  path: /ws-path
  headers: { Host: vpn.example.ru }
client-fingerprint: safari

# 4. Тот же WebSocket, но через CDN (Cloudflare и т. п.) — последний рубеж
- name: "WebSocket CDN"
  type: vless
  server: cdn.example.ru
  port: 443
  uuid: UUID
  network: ws
  tls: true
  udp: true
  servername: cdn.example.ru
  ws-opts:
    path: /ws-path
    headers: { Host: cdn.example.ru }
  client-fingerprint: safari

# 5. Необязательно: узел второго VPN-провайдера для видео (раздел 10)
- name: "Узел для видео"
  type: vless
  server: VIDEO_NODE
  port: 443
  uuid: UUID_2
  network: tcp
  tls: true
  udp: true
  servername: SNI_2
  client-fingerprint: firefox # как в подписке провайдера

proxy-groups:
- name: Proxy # сюда идёт всё, что не в исключениях
  type: select
  proxies: [Auto, "Reality (свой домен)", "Reality (резерв)", "WebSocket TLS", "WebSocket CDN"]
- name: Auto
  type: fallback # первый живой по порядку
  proxies: ["Reality (свой домен)", "Reality (резерв)", "WebSocket TLS", "WebSocket CDN"]
  url: http://www.gstatic.com/generate_204
  interval: 300 # проверка раз в 5 минут
- name: Video
  type: fallback # узел для видео, при сбое — свой сервер
  proxies: ["Узел для видео", Proxy]
  url: https://www.gstatic.com/generate_204 # только https: см. раздел 10
  interval: 300

```

Почему fallback, а не «самый быстрый» (url-test). При близкой задержке url-test иногда переключает сервер посреди загрузки, и видео и большие загрузки зависают. Fallback держит основной сервер, пока он жив.

ЧАСТЬ 3: ПРАВИЛА — ИСКЛЮЧЕНИЯ СВЕРХУ, ВСЁ ОСТАЛЬНОЕ В VPN

```

rules:
# провайдер и локальные сети
- DOMAIN-SUFFIX,provider.ru,DIRECT
- IP-CIDR,10.0.0.0/8,DIRECT,no-resolve
- IP-CIDR,100.64.0.0/10,DIRECT,no-resolve
- IP-CIDR,172.16.0.0/12,DIRECT,no-resolve
- IP-CIDR,192.168.0.0/16,DIRECT,no-resolve

```

```

# видеосервисы — через группу Video, сразу после локальных сетей
- DOMAIN-SUFFIX,video.example,Video
- DOMAIN-SUFFIX,video-cdn.example,Video
# госсервисы и магазины приложений
- DOMAIN-SUFFIX,gosuslugi.ru,DIRECT
- DOMAIN-SUFFIX,rustore.ru,DIRECT
# мессенджеры и соцсети
- DOMAIN-SUFFIX,max.ru,DIRECT
- DOMAIN-SUFFIX,oneme.ru,DIRECT
- DOMAIN-SUFFIX,vk.ru,DIRECT
- DOMAIN-SUFFIX,vk.com,DIRECT
- DOMAIN-SUFFIX,vkontakte.ru,DIRECT
- DOMAIN-SUFFIX,userapi.com,DIRECT
- DOMAIN-SUFFIX,vkuser.net,DIRECT
- DOMAIN-SUFFIX,vk-cdn.net,DIRECT
- DOMAIN-SUFFIX,mycdn.me,DIRECT
# маркетплейсы и объявления
- DOMAIN-SUFFIX,avito.ru,DIRECT
- DOMAIN-SUFFIX,avito.st,DIRECT
- DOMAIN-SUFFIX,ozon.ru,DIRECT
- DOMAIN-SUFFIX,ozone.ru,DIRECT
- DOMAIN-SUFFIX,ozon.com,DIRECT
- DOMAIN-SUFFIX,ozonusercontent.com,DIRECT
- DOMAIN-SUFFIX,wildberries.ru,DIRECT
- DOMAIN-SUFFIX,wb.ru,DIRECT
- DOMAIN-SUFFIX,wbasket.ru,DIRECT
- DOMAIN-SUFFIX,wbstatic.net,DIRECT
- DOMAIN-SUFFIX,wbcontent.net,DIRECT
# карты и поиск
- DOMAIN-SUFFIX,2gis.ru,DIRECT
- DOMAIN-SUFFIX,2gis.com,DIRECT
- DOMAIN-SUFFIX,yandex.ru,DIRECT
- DOMAIN-SUFFIX,yandex.net,DIRECT
- DOMAIN-SUFFIX,yandex.com,DIRECT
- DOMAIN-SUFFIX,ya.ru,DIRECT
- DOMAIN-SUFFIX,yastatic.net,DIRECT
- DOMAIN-SUFFIX,yandexcloud.net,DIRECT
# банки
- DOMAIN-SUFFIX,sberbank.ru,DIRECT
- DOMAIN-SUFFIX,sber.ru,DIRECT
- DOMAIN-SUFFIX,sberbank.com,DIRECT
- DOMAIN-SUFFIX,sbrf.ru,DIRECT
# IP-телефония: домены + подсети серверов (голос идёт по IP без имени сайта)
- DOMAIN-SUFFIX,novofon.com,DIRECT
- DOMAIN-SUFFIX,novofon.ru,DIRECT
- DOMAIN-SUFFIX,mango-office.ru,DIRECT
- DOMAIN-SUFFIX,mango-office.com,DIRECT
- DOMAIN-SUFFIX,mangosip.ru,DIRECT
- IP-CIDR,37.139.38.0/24,DIRECT,no-resolve # Новофон
- IP-CIDR,81.88.85.0/24,DIRECT,no-resolve # Манго Офис
- IP-CIDR,81.88.86.0/24,DIRECT,no-resolve # Манго Офис
# телевизор: медиаприложение и его CDN (раздел 11)
- DOMAIN-SUFFIX,vkvideo.ru,DIRECT
- DOMAIN-SUFFIX,okcdn.ru,DIRECT
- AND,((SRC-IP-CIDR,192.168.8.50/32),(DOMAIN-KEYWORD,app-name)),DIRECT
# мессенджеры остаются в VPN — ОБЯЗАТЕЛЬНО выше правила больших загрузок
- IP-CIDR,91.108.0.0/16,Proxy,no-resolve # Telegram
- IP-CIDR,149.154.160.0/20,Proxy,no-resolve # Telegram
- IP-CIDR,95.161.64.0/20,Proxy,no-resolve # Telegram
- IP-CIDR,185.76.151.0/24,Proxy,no-resolve # Telegram
- DOMAIN-SUFFIX,telegram.org,Proxy
- DOMAIN-SUFFIX,t.me,Proxy
- DST-PORT,3478-3481,Proxy # STUN: звонки в мессенджерах
# большие загрузки (торрент-клиенты, обновления) — напрямую по портам
- AND,((DST-PORT,1024-65535),(NOT,((DST-PORT,5222/5223/5228/8080/8443/8880)))),DIRECT

```

```
# всё остальное — через VPN. Эта строка всегда последняя.  
- MATCH,Прoxy
```

ПРОВЕРКА КОНФИГА ПЕРЕД ЗАПУСКОМ

```
chmod 600 /etc/mihomo/config.yaml # внутри ключи — только для root  
mihomo -d /etc/mihomo -t          # «configuration file ... test is successful»
```

Подсети телефонии — пример, а не истина. Провайдеры телефонии меняют адреса. Как найти актуальную подсеть по живому звонку — в разделе «Исключения».

07 · ШАГ 6

Служба и автозапуск

Скрипт запускает mihomo при загрузке, перезапускает при падении и при переподключении к провайдеру, а заодно ставит служебное правило маршрутизации.

/ETC/INIT.D/MIHOMO

```
#!/bin/sh /etc/rc.common  
# mihomo: весь трафик роутера и локальной сети — через TUN-интерфейс Meta.  
  
START=99  
STOP=10  
USE_PROCD=1  
  
# Фирменный модуль GL.iNet помечает трафик LAN меткой 0x8000 и правилом 6000  
# отправляет его в основную таблицу раньше правил mihomo (9000+) — LAN уходит  
# мимо туннеля. Правило 5990 направляет LAN в таблицу mihomo (2022) раньше.  
lan_rule() {  
    ip rule del pref 5990 2>/dev/null  
    [ "$1" = add ] && ip rule add pref 5990 iif br-lan lookup 2022  
}  
  
start_service() {  
    lan_rule add  
    procd_open_instance  
    procd_set_param command /usr/bin/mihomo -d /etc/mihomo  
    procd_set_param respawn 3600 5 0  
    procd_set_param limits nofile="65535 65535"  
    procd_set_param stdout 1  
    procd_set_param stderr 1  
    procd_close_instance  
}  
  
stop_service() {  
    lan_rule del  
}  
  
service_triggers() {  
    procd_add_interface_trigger "interface.*.up" wan /etc/init.d/mihomo restart  
}
```

```
chmod +x /etc/init.d/mihomo  
/etc/init.d/mihomo enable  
/etc/init.d/mihomo start  
/etc/init.d/mihomo status          # running
```

```
ip -br addr show Meta          # интерфейс туннеля поднят
ip rule | grep -E '^5990|^6000' # 5990 должно стоять ВЫШЕ 6000
```

Без правила 5990 схема выглядит рабочей, но не работает. Сам роутер выходит в интернет через VPN, а компьютеры в сети — напрямую через провайдера. Поэтому внешний IP всегда проверяйте с устройства в локальной сети (шаг 8).

08 · Ш А Г 7

Брандмауэр и DNS

Туннелю нужна своя зона в брандмауэре, а DNS-запросы устройств должны попадать в `mihome` — иначе он не узнает имя сайта и исключения не сработают.

7.1 Зона брандмауэра для туннеля

```
uci set firewall.mihome=zone
uci set firewall.mihome.name='mihome'
uci set firewall.mihome.device='Meta'
uci set firewall.mihome.input='ACCEPT'
uci set firewall.mihome.output='ACCEPT'
uci set firewall.mihome.forward='ACCEPT'

uci set firewall.lan_mihome=forwarding
uci set firewall.lan_mihome.src='lan'
uci set firewall.lan_mihome.dest='mihome'

uci commit firewall
/etc/init.d/firewall reload
```

7.2 dnsmasq отправляет запросы в mihome

```
uci set dhcp.@dnsmasq[0].noresolv='1'
uci add_list dhcp.@dnsmasq[0].server='127.0.0.1#1053'
uci commit dhcp
/etc/init.d/dnsmasq restart

# проверка: ответ должен прийти из диапазона fake-ip 198.18.x.x
nslookup google.com 127.0.0.1
```

Если на компьютере работает свой Clash Verge, у него тот же диапазон `fake-ip 198.18.0.0/16`. Пока Clash на компьютере включён, адреса, выданные роутером, компьютер отправит в свой Clash. Для проверки роутера выключите Clash на компьютере.

09 · Ш А Г 8

Проверка

Проверяем с роутера и обязательно с устройства в сети.

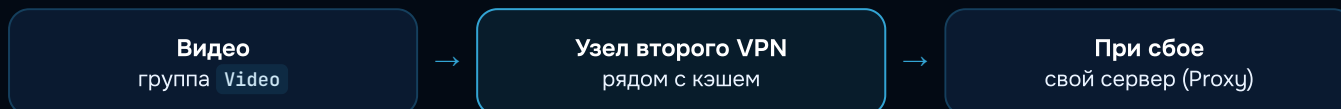
```
# 1. С роутера: внешний IP – страна вашего VPN-сервера
curl -s https://ipinfo.io/json

# 2. Какой сервер выбран и отклик всех серверов
S=$(grep ^secret /etc/mihomo/config.yaml | cut -d' ' -f2)
curl -s -H "Authorization: Bearer $S" http://192.168.8.1:9090/proxies/Auto | grep -o '"now": "[^"]*"'
curl -s -H "Authorization: Bearer $S" "http://192.168.8.1:9090/group/Auto/delay?url=http://www.gstatic.com/generate_204&timeout=8000"
```

1. С компьютера или телефона в сети роутера откройте `ipinfo.io` : должна быть страна VPN-сервера.
2. Откройте сайт из исключений, например `2ip.ru` через Яндекс или личный кабинет банка: банк не должен просить дополнительных подтверждений.
3. Сделайте **тестовый звонок** через IP-телефонию: должно быть слышно обе стороны, без эха.
4. Перезагрузите роутер (`reboot`) и повторите пункт 1: служба должна подняться сама.

Два VPN: отдельный узел для видео

Разные сервисы — через разные выходы. Свой сервер в Европе даёт полный контроль, но он далеко от видеокэша. Узел второго VPN-провайдера в России ближе к кэшу и отдаёт видео с минимальной задержкой.



10.1 Откуда взять настройки узла

Если у вас уже есть подписка второго провайдера в Clash Verge, узел целиком лежит в файле профиля: **Профили** → **Редактировать файл**, раздел `proxies`. Скопируйте нужный узел в конфиг роутера как пятый сервер (часть 2 конфига) и добавьте группу `Video`. Отпечаток (`client-fingerprint`) оставьте таким, как в подписке.

Чтобы не копировать руками после каждого обновления подписки, удобен короткий скрипт. Он читает конфиг роутера и профиль Clash Verge, переносит один узел и пересобирает группу и правила. Подписка обновилась — запускаете скрипт ещё раз.

```
# add_video_group.py — запуск на компьютере:
# ssh root@192.168.8.1 cat /etc/mihomo/config.yaml | python add_video_group.py > new.yaml
import os, sys, yaml
NODE = "Название узла в подписке"
PROFILE = r"%APPDATA%\io.github.clash-verge-rev\profiles\ФАЙЛ.yaml"
DOMAINS = ["video.example", "video-cdn.example"]

cfg = yaml.safe_load(sys.stdin.read())
sub = yaml.safe_load(open(os.path.expandvars(PROFILE), encoding="utf-8"))
src = next(p for p in sub["proxies"] if p["name"] == NODE)

cfg["proxies"] = [p for p in cfg["proxies"] if p["name"] != "Узел для видео"]
cfg["proxies"].append(dict(src, name="Узел для видео"))
cfg["proxy-groups"] = [g for g in cfg["proxy-groups"] if g["name"] != "Video"]
cfg["proxy-groups"].append({"name": "Video", "type": "fallback",
    "proxies": ["Узел для видео", "Proxy"],
    "url": "https://www.gstatic.com/generate_204", "interval": 300})
rules = [r for r in cfg["rules"] if not r.endswith(",Video")]
pos = max(i for i, r in enumerate(rules) if r.startswith("IP-CIDR,192.168.0.0/16")) + 1
rules[pos:pos] = [f"DOMAIN-SUFFIX,{d},Video" for d in DOMAINS]
cfg["rules"] = rules
yaml.safe_dump(cfg, sys.stdout, allow_unicode=True, sort_keys=False)
```

```
# передать на роутер, проверить и применить
cat new.yaml | ssh root@192.168.8.1 "cp /etc/mihomo/config.yaml /etc/mihomo/config.yaml.bak; cat >
/etc/mihomo/config.yaml"
ssh root@192.168.8.1 "mihomo -d /etc/mihomo -t && /etc/init.d/mihomo restart"
```

10.2 Как проверить

Видеосервис Google показывает, с какого IP он видит роутер и какой кэш отдаёт видео. Запустите с роутера:

```
curl -s "https://redirector.googlevideo.com/report_mapping?di=no"
# в ответе — внешний IP узла и имя кэша; у нас был московский кэш sv004
```

Проверку группы Video — только по https. Узел второго провайдера может не пропускать обычный HTTP: у нас проверка по `http://www.gstatic.com/generate_204` уходила в таймаут, и fallback считал узел мёртвым — видео всё время шло через свой сервер, хотя узел работал. С `https://` узел отвечает. Проверить: `curl -s -H "Authorization: Bearer $S" "http://192.168.8.1:9090/proxies/Video"` — в поле `now` должен стоять узел, а не `Proxy`.

Правила для видео — сразу после локальных сетей. Правила читаются сверху вниз. Если домен видео окажется ниже правила больших загрузок или `MATCH`, группа не работает.

Без второго провайдера раздел можно пропустить: тогда видео идёт через ваш сервер вместе со всем остальным. Группа `Video` с запасным выходом `Proxy` всё равно полезна — узел можно добавить позже, не трогая правила.

11

Исключения: что пускать напрямую

Через VPN идёт всё, кроме списка исключений. Без них неудобства начинаются сразу.

СЕРВИС	ЧТО БУДЕТ ЧЕРЕЗ VPN
Банки	Зарубежный IP включает антифрод: дополнительные проверки, блокировка операций
Маркетплейсы, карты	Не тот город, не те цены и сроки доставки
IP-телефония	Лишние 50–100 мс задержки, эхо, одностороннее аудио
Госуслуги, RuStore, ВКонтакте	Медленнее, иногда ограничения по доступу

Правила, которые стоит знать

- `DOMAIN-SUFFIX` действует на домен и все его поддомены: `vk.com` покрывает и `m.vk.com`.
- Добавляйте служебные домены.** ВКонтакте отдаёт картинки и видео с `userapi.com`, `vkuser.net`, `mycdn.me` — без них лента грузится наполовину. Ozon — с `ozonusercontent.com`, Wildberries — с `wbbasket.ru` и `wbstatic.net`.
- Правила читаются сверху вниз до первого совпадения, поэтому `MATCH`, `Proxy` — всегда последняя строка.
- Для подсетей пишите `no-resolve`: тогда mihomo не будет делать лишний DNS-запрос.

Добавить исключение

```
D=example.ru
grep -q "^- DOMAIN-SUFFIX,$D,DIRECT$" /etc/mihomo/config.yaml || \
  sed -i "/^- MATCH,Proxy$/i - DOMAIN-SUFFIX,$D,DIRECT" /etc/mihomo/config.yaml
mihomo -d /etc/mihomo -t && /etc/init.d/mihomo restart
```

```
# подсеть — так же, строкой вида:
# - IP-CIDR,1.2.3.0/24,DIRECT,no-resolve
```

Как найти адрес для телефонии

Правило по домену голос не ловит: звук идёт по UDP прямо на IP-адреса серверов телефонии. Признаком, что подсеть пропущена, — в звонке слышно только одну сторону. Сделайте звонок и посмотрите, куда уходят UDP-соединения и через какое правило:

```
S=$(grep ^secret /etc/mihomo/config.yaml | cut -d' ' -f2)
curl -s -H "Authorization: Bearer $S" http://192.168.8.1:9090/connections \
  | grep -o '"network":"udp"[^]*"destinationIP":"[^"]*" ' | sort -u
# адрес, ушедший в Проху, превратите в подсеть /24 и добавьте исключением
```

Большие загрузки мимо VPN

Торрент-клиент, обновления системы или дистрибутивы забивают канал VPN-сервера, и остальным устройствам достаются крошки. mihomo не распознаёт такой трафик по содержимому, поэтому правило строится по портам: всё, что идёт на порты 1024–65535, — напрямую. Стандартные порты, на которых работают сайты, остаются в VPN.

```
- AND, ((DST-PORT, 1024-65535), (NOT, ((DST-PORT, 5222/5223/5228/8080/8443/8880)))) , DIRECT
# кроме пушей Google (5228), XMPP (5222/5223) и запасных HTTP/HTTPS-портов
```

Главная грабля — мессенджеры. Под это правило попадают звонки: Telegram ходит на порт 20443, STUN — на 3478–3481. Первая версия правила отправила Telegram напрямую — это сразу видно по списку соединений. Поэтому подсети и домены мессенджеров и порты STUN стоят **выше** правила, с выходом **Проху** (часть 3 конфига). Если какое-то приложение на нестандартном порту перестало работать, добавьте его домен с **Proxy** выше строки **AND**.

Какое правило сработало для каждого соединения, показывает список соединений:

```
curl -s -H "Authorization: Bearer $S" http://192.168.8.1:9090/connections \
  | grep -o '"host":"[^"]*"rule":"[^"]*",rulePayload":"[^"]*" ' | sort -u | head -40
```

Телевизор и медиаприложения

Закрепите за телевизором постоянный адрес. Правила для конкретного устройства (**SRC-IP-CIDR**) держатся на его IP. Без закрепления роутер однажды выдаст другой адрес, и правила молча перестанут работать.

```
uci add dhcp host
uci set dhcp.@host[-1].name='android-tv'
uci set dhcp.@host[-1].mac='TV_MAC'
uci set dhcp.@host[-1].ip='192.168.8.50'
uci commit dhcp
/etc/init.d/dnsmasq restart
# переключите телевизор к Wi-Fi, чтобы он получил новый адрес
```

Медиаприложения ходят не туда, куда думаешь. У нас приложение онлайн-кинотеатра брало видео не со своих серверов, а с CDN VK. Пока это не нашли, через VPN прошло около 420 МБ одного фильма. Приём работает для любого приложения: включите фильм и 10–15 минут записывайте соединения телевизора, затем добавьте найденные домены в исключения.

```
# раз в 30 секунд, 15 минут: к каким доменам ходит телевизор и через какой выход
for i in $(seq 1 30); do
  curl -s -H "Authorization: Bearer $S" http://192.168.8.1:9090/connections \
    | grep -o '"sourceIP":"192.168.8.50"[^]*"host":"[^"]*"' | grep -o '"host":"[^"]*"'
  sleep 30
done | sort | uniq -c | sort -rn | head -30
```

Домены, которые ушли в `Proxy`, а должны идти напрямую, добавьте как обычные исключения. Если у приложения много поддоменов с общим словом в имени, удобнее одно правило только для телевизора: `AND, ((SRC-IP-CIDR, 192.168.8.50/32), (DOMAIN-KEYWORD, app-name)), DIRECT`.

12

Обслуживание и безопасность

Все команды — на роутере: `ssh root@192.168.8.1`.

```
# состояние службы и туннеля
/etc/init.d/mihomo status; ip -br addr show Meta; ip rule | grep -E '^5990|^6000'
# перезапуск
/etc/init.d/mihomo restart
# логи
logread -e mihomo | tail -30
# текущие соединения: куда идут и по какому правилу
S=$(grep ^secret /etc/mihomo/config.yaml | cut -d' ' -f2)
curl -s -H "Authorization: Bearer $S" http://192.168.8.1:9090/connections
```

Временно выключить VPN

```
/etc/init.d/mihomo stop
uci delete dhcp.@dnsmasq[0].noresolv
uci del_list dhcp.@dnsmasq[0].server='127.0.0.1#1053'
uci commit dhcp
/etc/init.d/dnsmasq restart
```

Пока VPN выключен, роутер раздаёт обычный интернет провайдера. Включить обратно: верните две настройки dnsmasq (шаг 7.2), затем `/etc/init.d/mihomo start` и `/etc/init.d/dnsmasq restart`.

Обновить mihomo

```
# на компьютере: скачать новую сборку linux-arm64 и передать
scp -O mihomo-linux-arm64-vX.Y.Z.gz root@192.168.8.1:/tmp/mihomo.gz
# на роутере
cp /usr/bin/mihomo /tmp/mihomo.old
gunzip -c /tmp/mihomo.gz > /usr/bin/mihomo && chmod +x /usr/bin/mihomo
mihomo -d /etc/mihomo -t && /etc/init.d/mihomo restart
# откат: cp /tmp/mihomo.old /usr/bin/mihomo && /etc/init.d/mihomo restart
```

Удалить полностью

```
/etc/init.d/mihomo stop
/etc/init.d/mihomo disable
rm -rf /usr/bin/mihomo /etc/mihomo /etc/init.d/mihomo
uci delete firewall.mihomo
uci delete firewall.lan_mihomo
uci commit firewall
/etc/init.d/firewall reload
# затем верните dnsmasq, как в «Временно выключить VPN»
```

Безопасность после настройки

- ☐ Смените заводской пароль Wi-Fi с наклейки.
- ☐ Задайте сложный пароль администратора и не открывайте панель роутера из интернета.
- ☐ Вход по SSH — только по ключу.
- ☐ Гостевая сеть для посетителей — отдельно от офисной.
- ☐ Панель mihomo (порт 9090) доступна только из локальной сети и закрыта паролем **SECRET**.
- ☐ Документация с командами отката хранится рядом с роутером.

Держите рядом с роутером README. Где лежат конфиги, как добавить исключение, как выключить VPN — чтобы обслуживать сеть мог не только тот, кто её настраивал. Копию удобно положить прямо на роутер: `/etc/mihomo/README.md`.

Грабли и диагностика

Всё, на что мы наступили при настройке, — с признаками и решением.

ПРИЗНАК	ПРИЧИНА	ЧТО СДЕЛАТЬ
Роутер долго висит в «Connecting...»	Провайдер подключает по PPPoE, а не по DHCP	Шаг 2: выбрать PPPoE, логин и пароль из договора
Роутер выходит через VPN, а компьютеры в сети — напрямую	Фирменный модуль GL.iNet уводит LAN-трафик правилом 6000 мимо туннеля	Шаг 6: правило 5990 в init-скрипте; проверка <code>ip rule</code>
Основной сервер не подключается, остальные работают	Фильтр провайдера обрывает TLS, если имя сайта (SNI) не «родное» для IP сервера	Отдельный вход Reality с SNI собственного домена на этом же сервере; неавторизованные подключения отдаются локальному nginx с настоящим сертификатом
Подключение с одних серверов обрывается на рукопожатии	Отпечаток Chrome (большой ClientHello с постквантовым ключом) режется фильтром	<code>client-fingerprint: safari</code> у всех серверов
Тяжёлые сайты зависают посреди загрузки	Режим url-test переключает сервер при близкой задержке	Группа <code>type: fallback</code>
Таймаут как при блокировке, хотя сервер жив	Панель x-ui молча убирает из конфигурации клиентов с истёкшим сроком	Проверьте срок клиента; в логе сервера — <code>invalid request user id</code>
VPN не поднимается сразу после включения	Роутер не знает точного времени — сертификаты не проверяются	<code>ntpd -q -p 0.openwrt.pool.ntp.org</code>
Формы LuCI не сохраняются	Адрес <code>/ubus</code> перехвачен панелью GL.iNet	Менять настройки по SSH через <code>uci</code>
Сайт из исключений идёт через VPN	Устройство ходит в DNS мимо роутера, или не хватает служебного домена	Sniffer включён; посмотреть <code>/connections</code> , добавить домен
В звонке слышно одну сторону	Голос ушёл на IP вне исключённых подсетей	Раздел 11: найти адрес в <code>/connections</code> , добавить подсеть
Основной вход Reality то подключается, то нет	Фильтр провайдера пропускает и свой домен не всегда: у нас прошли 2 проверки из 3	Держать запасные серверы на WebSocket: fallback переключится сам и вернётся, когда основной оживёт
Видео всё время идёт через свой сервер, хотя узел для видео работает	Узел не пропускает проверку по HTTP, fallback считает его мёртвым	У группы Video <code>url:</code> <code>https://www.gstatic.com/generate_204</code>
Звонки в мессенджере не проходят после правила больших загрузок	Звонки идут на нестандартные порты и попали в DIRECT	Подсети и домены мессенджеров и STUN 3478-3481 — с <code>Proxy</code> выше правила <code>AND</code>
На телевизоре фильм идёт через VPN	Видео берётся с чужого CDN, а не с серверов приложения	Записать соединения телевизора за 10-15 минут (раздел 11), добавить домены CDN

Правила для телевизора
перестали работать

Телевизор получил другой IP

Закрепить адрес в DHCP по MAC

Компьютер теряет интернет при
подключении кабеля к роутеру

Windows сделала кабель
основным маршрутом

Метрика 500 у Ethernet (шаг 1)

Чек-лист

Перед покупкой и настройкой

- ☐ Роутер с OpenWrt, от 256 МБ ОЗУ и 128 МБ флеш
- ☐ Свой VPN-сервер, минимум два протокола
- ☐ Тип подключения провайдера и данные PPPoE
- ☐ Список российских сервисов, которыми пользуетесь
- ☐ Компьютер с OpenSSH и патч-корд

После настройки

- ☐ Заводской пароль Wi-Fi сменён
- ☐ Внешний IP проверен с устройства в сети
- ☐ Сайт из исключений и банк открываются напрямую
- ☐ Тестовый звонок: слышно обе стороны
- ☐ После перезагрузки VPN поднялся сам
- ☐ Звонок в мессенджере проходит после правила больших загрузок
- ☐ За телевизором закреплён адрес
- ☐ README с конфигами и командами лежит рядом



Успешный блог

Настрою роутер для вашего офиса под ключ

Роутер, VPN, исключения под ваши сервисы и документация для того, кто будет обслуживать сеть.
Напишите в Telegram [@uspeshnyy](https://t.me/uspeshnyy) · статья с разбором — blog.uspeshnyy.ru