????????? BGP (Antifilter) ????? Wireguard ?? Mikrotik (RouterOS 7)

Данное руководство описывает типовые проблемы и чек-лист настройки при маршрутизации заблокированного трафика через списки BGP (Antifilter) с использованием туннеля Wireguard.

Примечание: Инструкция подразумевает, что удаленный VPS-сервер (Wireguard, NAT) настроен корректно, работает штатно и готов к приему трафика.

????????? ????????? ? ?? ??????? (RouterOS 7)

1. ?????? ?? ????? ????????????? (Routing Loop)

Симптом: При включении BGP туннель Wireguard моментально падает, связь с роутером может обрываться. Маршруты то появляются, то пропадают.

Причина: По BGP прилетает маршрут до публичного IP вашего же VPS. Микротик пытается отправить служебный зашифрованный трафик Wireguard внутрь самого туннеля Wireguard (так как туда теперь направлен маршрут), из-за чего туннель схлопывается.

Что делать: Жестко привязать публичный IP VPS-сервера к физическому интерфейсу провайдера (WAN). Это исключит его попадание в туннель.

```
/ip route add dst-address=[ПУБЛИЧНЫЙ_IP_VPS]/32 gateway=ether1-WAN comment="Anti-Loop for WG"
```

(Замените `ether1-WAN` на имя вашего интерфейса с интернетом, например `pppoe-out1`).

2. ?????????? ??????? BGP (??????????? ?? ???????????? ID)

Симптом: Трафик не идет в туннель вообще, либо уходит в интернет напрямую. В настройках фильтров стоит шлюз вида `*0xa`.

Причина: В RouterOS 7 фильтры часто создаются через консоль или Winbox с указанием внутреннего шестнадцатеричного ID интерфейса (например, `*0xa`). При минорном обновлении прошивки, добавлении интерфейсов или перезагрузке этот внутренний ID меняется, и правило начинает указывать "в никуда".

Что делать: В фильтрах (Routing -> Filters) **всегда** прописывать текстовое имя интерфейса.

- ❌ Неправильно: `set gw *0xa; accept;`
- ✅ Правильно: `set gw WG0; accept;`

```
/routing/filter/rule/set [find chain=BGP_IN] rule="set gw WG0; accept;"
```

3. ????? ?????????? BGP-?????? ??????????? (BGP over VPN)

Симптом: BGP-сессия не поднимается (висит в статусе Connect/Active), маршруты не прилетают. Пинг до серверов Antifilter не проходит.

Причина: Провайдер (или ТСПУ) блокирует BGP-трафик (порт TCP 179) к известным серверам Antifilter.

Что делать: Спрятать саму BGP-сессию внутрь зашифрованного Wireguard-туннеля.

1. Направляем трафик до BGP-пира внутрь туннеля WG (чтобы запросы шли через VPN):
   ```
   /ip route add dst-address=[IP_СЕРВЕРА_BGP]/32 gateway=WG0 comment="BGP over WG"
   ```
2. В настройках BGP Connection (Routing -> BGP) меняем `local.address` с внешнего IP роутера на **внутренний IP Микротика в сети Wireguard** (например, 10.199.126.5). Иначе Mikrotik будет стучаться внешним адресом изнутри VPN:
   ```
   /routing/bgp/connection/set [find name="antifilter"] local.address=10.199.126.5
   ```

4. ???????? NAT (???????????) ?? Mikrotik

Симптом: BGP поднят, маршруты в таблице есть. Трассировка показывает, что пакеты уходят в туннель, но сайты не открываются (ответы не возвращаются).

Причина: Пакеты из домашней локальной сети уходят на VPS с серыми IP-адресами (например, 192.168.88.x). Удаленный сервер не может их замаскировать, так как его NAT

обычно настроен только на подсеть самого Wireguard (10.x.x.x).

Что делать: Убедиться, что на Микротике есть правило NAT, маскирующее локальный трафик при выходе в интерфейс Wireguard.

```
/ip firewall nat add chain=srcnat action=masquerade out-interface=WG0 comment="NAT for WG"
```

? ???-???? ??? ????????????

- [ ] **Связь с VPS:** Wireguard-туннель поднят? Пингуется ли внутренний IP VPS (например, 10.199.126.1) с Микротика?
- [ ] **Защита от петель (Routing Loop):** Прописан ли статический маршрут `/32` до публичного IP VPS-сервера через физический интерфейс провайдера (WAN)?
- [ ] **Имена интерфейсов в фильтрах:** В меню `Routing -> Filters` указано явное имя `WG0` вместо системных ID (`*0x...`)?
- [ ] **Защита BGP от блокировки:** Маршрутизируется ли IP-адрес BGP-сервера (например, 165.22.x.x) через интерфейс `WG0`?
- [ ] **Локальный IP для BGP:** В настройках сессии `Routing -> BGP` в поле `local.address` указан внутренний IP-адрес интерфейса `WG0` (а не внешний IP провайдера)?
- [ ] **Локальный NAT:** Включен ли `masquerade` (srcnat) для трафика, покидающего интерфейс `WG0`?

? ??????? ??? ???????????? (???????? ?? MIKROTIK)

Чтобы убедиться, что все настроено правильно, выполните следующие проверки через терминал (New Terminal) в Winbox.

1. ???????? ?????? ?????? ??????? Wireguard

Для начала нужно убедиться, что туннель поднят и данные бегают. Пингуем внутренний IP-адрес вашего VPS-сервера (в примере — `10.199.126.1`):

```
/ping 10.199.126.1 count=4
```

Ожидаемый результат: Пинги возвращаются (packet-loss=0%). Если таймаут — проблема в ключах, портах или Endpoint-адресе WG.

2. ???????? ????? ? BGP-???????? ????? ???????

Пингуем IP-адрес BGP-сервера Antifilter (в примере — резервный сервер `165.22.127.207`). Этот запрос должен идти строго внутри Wireguard.

```
/ping 165.22.127.207 count=4
```

Ожидаемый результат: Пинги идут. Если 100% потерь — вы забыли прописать статический маршрут до BGP-сервера через `WG0`, и трафик блокируется провайдером.

3. ???????? ??????? BGP-?????? ? ?????????

Проверяем, поднялась ли сессия и сколько маршрутов прилетело:

```
/routing/bgp/connection/print
/ip/route/print count-only where bgp
```

Ожидаемый результат: Сессия должна быть в статусе `established` (буква E), а вторая команда должна вывести количество полученных маршрутов (обычно около 30 000 — 45 000).

4. ??????????? ???????? (Traceroute) ?? ???????????????? ?????

Проверяем, каким путем роутер отправляет трафик к заблокированным ресурсам (для примера берем IP-адрес Cloudflare, за которым скрывается Rutracker — `104.21.32.39`):

```
/tool traceroute 104.21.32.39
```

Ожидаемый результат:
1-й хоп (прыжок) должен быть внутренним IP-адресом вашего VPS в сети Wireguard (например, `10.199.126.1`).
2-й хоп должен быть шлюзом провайдера вашего VPS-сервера.
Если первым хопом выступает IP-адрес вашего домашнего провайдера — маршруты BGP не применились.

5. ????????? ??????? ?? ????????? ???? (???????? NAT)

Если с самого Микротика пинг до заблокированного ресурса идет, а с телефонов/ноутбуков — нет, скорее всего, проблема в NAT. Имитируем запрос от имени домашнего устройства (замените `192.168.88.1` на IP-адрес вашего роутера в локальной сети):

```
/ping 104.21.32.39 src-address=192.168.88.1 count=4
```

Ожидаемый результат: Пинг должен пройти успешно. Если таймаут — на Микротике отсутствует или не работает правило `src-nat (masquerade)` для интерфейса `WG0`.

Revision #3
Created 4 June 2026 00:27:22 by Admin
Updated 4 June 2026 00:33:21 by Admin