Проверяем работу туннеля:

**PC1> ping 172.16.2.3 -c 3 -2**

**84 bytes from 172.16.2.3 udp\_seq=1 ttl=62 time=3.470 ms**

**84 bytes from 172.16.2.3 udp\_seq=2 ttl=62 time=9.277 ms**

**84 bytes from 172.16.2.3 udp\_seq=3 ttl=62 time=7.031 ms**

**PC1> trace 172.16.2.3**

**trace to 172.16.2.3, 8 hops max, press Ctrl+C to stop**

**1 172.16.1.1 4.572 ms 2.129 ms 3.724 ms**

**2 192.168.100.2 6.968 ms 5.508 ms 4.352 ms**

**3 \*172.16.2.3 5.147 ms (ICMP type:3, code:3, Destination port unreachable)**

C PC1 пакеты проходят через туннель.

**PC4> ping 172.16.1.3 -c 3 -2**

**84 bytes from 172.16.1.3 udp\_seq=1 ttl=62 time=6.795 ms**

**84 bytes from 172.16.1.3 udp\_seq=2 ttl=62 time=8.171 ms**

**84 bytes from 172.16.1.3 udp\_seq=3 ttl=62 time=6.030 ms**

**PC4> trace 172.16.1.4**

**trace to 172.16.1.4, 8 hops max, press Ctrl+C to stop**

**1 172.16.2.1 2.726 ms 3.173 ms 1.623 ms**

**2 10.10.10.2 5.034 ms 3.442 ms 3.723 ms**

**3 \*172.16.1.4 2.463 ms (ICMP type:3, code:3, Destination port unreachable)**

А вот с РС4 пакеты идут мимо тоннеля по физическому интерфесу Gi1/0/1 напрямую.

Смотрим конфиг на виртуальном роутере vesr-2 в части трансляции исходящих адресов пакетов:

nat source

  pool WAN

    ip address-range 10.10.20.2

  exit

  ruleset SNAT

    to zone UNTRUST

    rule 1

      match source-address object-group LAN\_NETWORK

**action source-nat pool WAN**

      enable

    exit

  exit

exit

Ошибка выделена рамкой и жирным шрифтом.

**Причина неправильной работы**

**Применение**

**action source-nat pool WAN**

**может привести к неправильной работе туннеля GRE**, потому что **туннель GRE использует для передачи трафика свой собственный интерфейс**, а правило NAT, привязанное к исходящему интерфейсу, не соответствует туннелированному пакету. [networkengineering.stackexchange.com](https://tr-page.yandex.ru/translate?lang=en-ru&url=https%3A%2F%2Fnetworkengineering.stackexchange.com%2Fquestions%2F70869%2Fcombining-nat-an-tunneling)

Это происходит из-за того, что туннель создаёт новый пакет с адресами внешнего туннеля, а правило NAT, привязанное к исходящему интерфейсу, не учитывает это преобразование. В результате туннель не получает трафик, предназначенный для него, и не может корректно работать. [networkengineering.stackexchange.com](https://tr-page.yandex.ru/translate?lang=en-ru&url=https%3A%2F%2Fnetworkengineering.stackexchange.com%2Fquestions%2F70869%2Fcombining-nat-an-tunneling)

Чтобы решить проблему, нужно изменить настройку NAT: использовать

action source-nat interface

 для преобразования IP-адреса отправителя на адрес туннельного интерфейса, а

action source-nat pool WAN

 — для выбора IP-адреса из пользовательского пула. [docs.eltex-co.ru](https://docs.eltex-co.ru/pages/viewpage.action?pageId=53817740)[juniper.net](https://www.juniper.net/documentation/us/en/software/junos/nat/topics/topic-map/nat-security-source-and-source-pool.html)[networkengineering.stackexchange.com](https://tr-page.yandex.ru/translate?lang=en-ru&url=https%3A%2F%2Fnetworkengineering.stackexchange.com%2Fquestions%2F70869%2Fcombining-nat-an-tunneling)

Исправляем на :

nat source

  pool WAN

    ip address-range 10.10.20.2

  exit

  ruleset SNAT

    to zone UNTRUST

    rule 1

      match source-address object-group LAN\_NETWORK

**action source-nat interface**

      enable

    exit

  exit

exit

**PC4> trace 172.16.1.3**

**trace to 172.16.1.3, 8 hops max, press Ctrl+C to stop**

**1 172.16.2.1 1.045 ms 2.672 ms 3.200 ms**

**2 192.168.100.1 5.909 ms 1.622 ms 3.208 ms**

**3 \*172.16.1.3 4.540 ms (ICMP type:3, code:3, Destination port unreachable)**