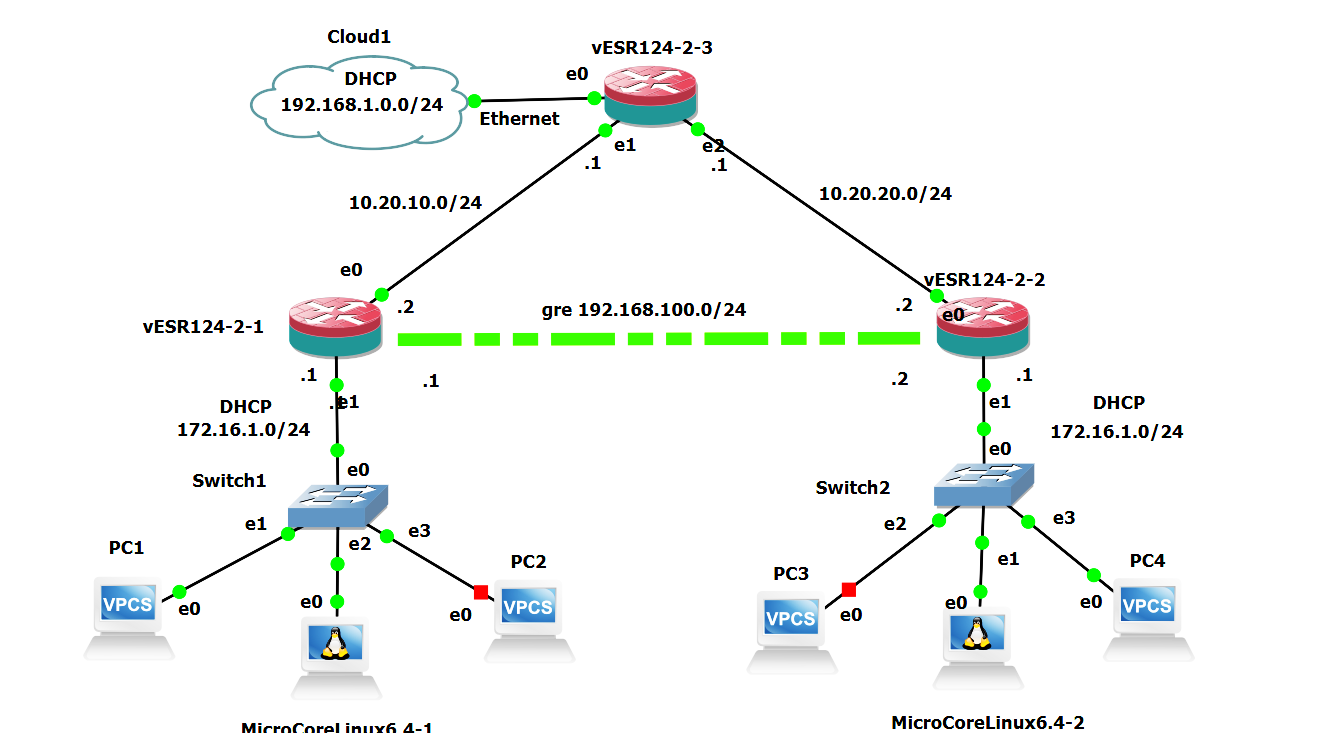
# Глава 8. Настройка GRE-over-IPSEC в маршрутизаторе vESR.

Цель:

создать условия защищенного соединения между удаленными офисами, центральным домашним и филиальным через Интернет с использованием топологии на схеме сети показанной на [Рис 7.1](Screens/Рис7-1.png). Подготовить виртуальный маршрутизатор vESR для работы в симуляторе GNS3 с для организации защищённого соединения тоннелем с использованием комбинации протоколов GRE и IPSEC.

[](Глава%208-GRE+IPSEC.docx)

**GRE (Generic Routing Encapsulation) применяется для туннелирования сетевых пакетов**. Он позволяет «завернуть» любой сетевой трафик (IP, не-IP, даже мультикаст) в отдельный туннель и передать его через сеть, которая этот трафик сама по себе не поддерживает. [ru.wikipedia.org\*](https://ru.wikipedia.org/wiki/GRE_%28%D0%BF%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB%29)[arenda-server.cloud](https://arenda-server.cloud/blog/seti-i-protokoly-chem-polezen-gre-tunnel/)

**Некоторые области применения GRE:**

* **Соединение частных сетей через интернет**. Например, если есть два офиса с приватной подсетью, а между ними только интернет. GRE позволяет «сшить» их в одну виртуальную сеть, даже если нет возможности поднять полноценный VPN.
* **Прокидывание нестандартных протоколов**. Некоторые протоколы (например, OSPF, EIGRP, мультикаст) не проходят через NAT или блокируются провайдерами. GRE-туннель позволяет «завернуть» их в IP-пакеты и передать через любую сеть.
* **Организация «серых» прокси и дорвеев**. GRE-туннели помогают подменить IP, быстро развернуть инфраструктуру для тестов, парсинга, обхода блокировок.
* **Разделение сетей и маршрутизация**. GRE позволяет строить сложные маршруты между дата-центрами, филиалами, облаками, когда стандартных средств мало или они неудобны.

Настройка GRE:

В vESR реализованы **статические неуправляемые GRE-туннели**, которые создаются вручную на локальном и удалённом узлах. Некоторые шаги для настройки:

* **Создание туннеля** с указанием IP-адресов интерфейсов, граничащих с WAN.
* **Назначение IP-адреса туннеля** на локальной стороне.
* **Принадлежность туннеля к зоне безопасности**, чтобы можно было создать правила для прохождения трафика в firewall.
* **Включение туннеля**.
* **Создание маршрута** до локальной сети партнёра, где в качестве интерфейса назначения указан ранее созданный туннель GRE.

[ELTEXcm.ru](https://eltexcm.ru/baza-znanij/esr/esr-nastrojka-gre-tunnelej.html)[mcgrp.ru](https://mcgrp.ru/files/viewer/154409/65)

Настройка IPSec:

Для защиты GRE-туннеля в vESR необходимо настроить **профиль параметров безопасности для IPSec-туннеля**. В профиле указываются алгоритм шифрования (например, AES 128 bit) и алгоритм аутентификации (например, MD5). [tenea.ru](https://tenea.ru/2024/03/20/%D1%81%D0%BE%D0%B7%D0%B4%D0%B0%D0%BD%D0%B8%D0%B5-%D0%B7%D0%B0%D1%89%D0%B8%D1%89%D0%B5%D0%BD%D0%BD%D0%BE%D0%B3%D0%BE-%D1%81%D0%BE%D0%B5%D0%B4%D0%B8%D0%BD%D0%B5%D0%BD%D0%B8%D1%8F-vesr/)[ELTEXcm.ru](https://eltexcm.ru/baza-znanij/esr/primer-nastrojki/tunnelirovanie/ipsec/esr-nastrojka-route-based-ipsec-vpn.html)

Также нужно создать **политику для IPSec-туннеля**, которая указывает список профилей, по которым могут согласовываться узлы. [tenea.ru](https://tenea.ru/2024/03/20/%D1%81%D0%BE%D0%B7%D0%B4%D0%B0%D0%BD%D0%B8%D0%B5-%D0%B7%D0%B0%D1%89%D0%B8%D1%89%D0%B5%D0%BD%D0%BD%D0%BE%D0%B3%D0%BE-%D1%81%D0%BE%D0%B5%D0%B4%D0%B8%D0%BD%D0%B5%D0%BD%D0%B8%D1%8F-vesr/)[ELTEXcm.ru](https://eltexcm.ru/baza-znanij/esr/primer-nastrojki/tunnelirovanie/ipsec/esr-nastrojka-route-based-ipsec-vpn.html)

После этого можно создать **IPSec-туннель**, указав шлюз IKE-протокола, политику IPSec-туннеля, режим обмена ключами и способ установления соединения. [tenea.ru](https://tenea.ru/2024/03/20/%D1%81%D0%BE%D0%B7%D0%B4%D0%B0%D0%BD%D0%B8%D0%B5-%D0%B7%D0%B0%D1%89%D0%B8%D1%89%D0%B5%D0%BD%D0%BD%D0%BE%D0%B3%D0%BE-%D1%81%D0%BE%D0%B5%D0%B4%D0%B8%D0%BD%D0%B5%D0%BD%D0%B8%D1%8F-vesr/)[ELTEXcm.ru](https://eltexcm.ru/baza-znanij/esr/primer-nastrojki/tunnelirovanie/ipsec/esr-nastrojka-route-based-ipsec-vpn.html). В документации ESR-series (например, версии 1.23) описан пример настройки **GRE over IPSec-туннеля** между двумя узлами. В конфигурации используются статические GRE-туннели и IPSec, при этом параметры туннеля для обеих сторон должны быть взаимосогласованными. [docs.eltex-co.ru](https://docs.eltex-co.ru/pages/viewpage.action?pageId=431915320)[docs.eltex-o.ru](https://docs.eltex-co.ru/pages/viewpage.action?pageId=55183533)[sysahelper.gitbook.io](https://sysahelper.gitbook.io/sysahelper/main/telecom/main/vesr_greoveripsec), в маршрутизаторе ESR реализованы статические неуправляемые GRE-туннели, то есть туннели создаются вручную путем конфигурирования на локальном и удаленном узлах.

Решение:

Для туннелирования трафика протокола GRE в настройках локального шлюза для туннеля используется IP-адрес 10.10.10.2, а в качестве удаленного шлюза для туннеля используется IP-адрес 10.10.20.2. IP-адрес самого туннеля на локальной стороне назначен 192.168.1.1/24. На стороне удаленного филиала IP адрес самого туннеля будет 192.168.1.2/24.

Проверяем сетевые настройки на виртуальных ПК PC1 и PC4 в локальных сетях 172.16.1.0/24 и 172.16.2.0/24 соответственно:

**PC1> ip dhcp**

**DDORA IP 172.16.1.4/24 GW 172.16.1.1**

**PC4> ip dhcp**

**DORA IP 172.16.2.3/24 GW 172.16.2.1**

Сервера DHCP работают и адреса машинами получены.

Проверяем работу Source NAT с выходом в Интернет:

**PC1> ping ya.ru**

**ya.ru resolved to 5.255.255.242**

**84 bytes from 5.255.255.242 icmp\_seq=1 ttl=246 time=11.277 ms**

**84 bytes from 5.255.255.242 icmp\_seq=2 ttl=246 time=14.373 ms**

**84 bytes from 5.255.255.242 icmp\_seq=3 ttl=246 time=17.397 ms**

**84 bytes from 5.255.255.242 icmp\_seq=4 ttl=246 time=14.769 ms**

**84 bytes from 5.255.255.242 icmp\_seq=5 ttl=246 time=18.071 ms**

**PC4> ping ya.ru**

**ya.ru resolved to 77.88.55.242**

**84 bytes from 77.88.55.242 icmp\_seq=1 ttl=50 time=15.720 ms**

**84 bytes from 77.88.55.242 icmp\_seq=2 ttl=50 time=19.953 ms**

**84 bytes from 77.88.55.242 icmp\_seq=3 ttl=50 time=19.831 ms**

**84 bytes from 77.88.55.242 icmp\_seq=4 ttl=50 time=31.104 ms**

**84 bytes from 77.88.55.242 icmp\_seq=5 ttl=50 time=19.792 ms**

Проверяем связность локальных сетей домашнего офиса и удаленного филиала, командой ping c PC4 у которой IP адрес 172.16.2.3 на PC1 у которой IP адрес 172.16.1.3:

**PC4> ping 172.16.1.3**

**172.16.1.3 icmp\_seq=1 timeout**

**172.16.1.3 icmp\_seq=2 timeout**

**172.16.1.3 icmp\_seq=3 timeout**

**172.16.1.3 icmp\_seq=4 timeout**

**172.16.1.3 icmp\_seq=5 timeout**

Вот для создания связности удаленных локальных сетей и нужен тоннель.

Создадим туннель GRE 10:

vesr-1(config)# tunnel gre 10

Укажем локальный и удаленный шлюз (IP-адреса интерфейсов, граничащих с WAN):

vesr-1(config-gre)# local address 10.10.10.2

vesr-1(config-gre)# remote address 10.10.20.20

Укажем IP-адрес туннеля 192.168.100.1/24:

vesr-1(config-gre)# ip address 192.168.100.1/24

Также туннель должен принадлежать к зоне безопасности, для того чтобы можно было

создать правила, разрешающие прохождение трафика в firewall. Принадлежность туннеля к зоне задается следующей командой:

vesr-1(config-gre)# security-zone UNTRUSTED

Включим туннель:

vesr-1(config-gre)# enable

vesr-1(config-gre)# exit

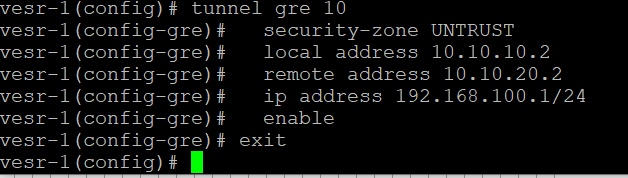


Рисунок 0.1. Экран терминала с конфигурацией туннеля.

Применяем настройки:

**vesr-1(config)# do commit**

**2025-06-19T10:48:28+00:00 %LINK-W-DOWN: gre 10 changed state to down**

**2025-06-19T10:48:28+00:00 %LINK-I-UP: gre 10 changed state to up**

**Configuration has been successfully applied and saved to flash. Commit timer started, changes will be reverted in 600 seconds.**

**2025-06-19T10:48:29+00:00 %CLI-I-CRIT: user admin from console input: do commit**

**vesr-1(config)# do confirm**

**Configuration has been confirmed. Commit timer canceled.**

**2025-06-19T10:48:32+00:00 %CLI-I-CRIT: user admin from console input: do confirm**

**vesr-1(config)#**

Повторяем эту настройку зеркально для виртуального маршрутизатора vesr-2:

vesr-2(config)# tunnel gre 10

Укажем локальный и удаленный шлюз (IP-адреса интерфейсов, граничащих с WAN):

vesr-2(config-gre)# local address 10.10.20.2

vesr-2(config-gre)# remote address 10.10.10.20

Укажем IP-адрес туннеля 192.168.100.2/24:

vesr-2(config-gre)# ip address 192.168.100.2/24

Также туннель должен принадлежать к зоне безопасности, для того чтобы можно было

создать правила, разрешающие прохождение трафика в firewall. Принадлежность туннеля к зоне задается следующей командой:

vesr-2(config-gre)# security-zone UNTRUSTED

Включим туннель:

vesr-2(config-gre)# enable

vesr-2(config-gre)# exit

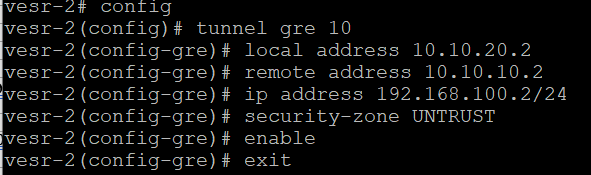


Рисунок 0.2. Экран терминала с конфигурацией туннеля.

Применяем настройки проверяем:

**vesr-1# sh ip int**

**IP address Interface Admin Link Type Precedence**

**--------------------------------------------------- -------------------- ----- ----- ------- -----------**

**10.10.10.2/24 gi1/0/1 Up Up static primary**

**172.16.1.1/24 gi1/0/2 Up Up static primary**

**192.168.100.1/24 gre 10 Up Up static primary**

**vesr-1# ping 192.168.100.2**

**PING 192.168.100.2 (192.168.100.2) 56 bytes of data.**

**!!!!!**

**--- 192.168.100.2 ping statistics ---**

**5 packets transmitted, 5 received, 0% packet loss, time 4011ms**

**rtt min/avg/max/mdev = 1.735/4.513/5.843/1.500 ms**

**vesr-1#**

**vesr-2# sh ip int**

**IP address Interface Admin Link Type Precedence**

**--------------------------------------------------- -------------------- ----- ----- ------- -----------**

**10.10.20.2/24 gi1/0/1 Up Up static primary**

**172.16.2.1/24 gi1/0/2 Up Up static primary**

**192.168.100.2/24 gre 10 Up Up static primary**

**vesr-2# ping 192.168.100.1**

**PING 192.168.100.1 (192.168.100.1) 56 bytes of data.**

**!!!!!**

**--- 192.168.100.1 ping statistics ---**

**5 packets transmitted, 5 received, 0% packet loss, time 4011ms**

**rtt min/avg/max/mdev = 3.188/4.423/7.256/1.462 ms**

**vesr-2#**

Туннель поднялся и доступен с обоих сторон.

Важно! Следует разрешить прохождение пакетов протокола GRE через файрволл на обоих сторонах.

security zone-pair UNTRUST self

rule 1

description "ICMP"

action permit

match protocol icmp

enable

exit

rule 2

description "GRE"

action permit

match protocol gre

enable

exit

Для удобство наблюдения за трассой прохождения пакетов IP необходимо разрешить traceroute в файрволле на обоих сторонах топологии:

Создается группа для сервиса traceroute:

**vesr-1# config**

**vesr-1(config)# object-group service TRACEROUTE**

**vesr-1(config-object-group-service)# port-range 33434-33534**

**vesr-1(config-object-group-service)# exit**

И добавляем еще несколько правил в работу файвола:

Для зоны UNTRUST self

**vesr-1(config)# security zone-pair UNTRUST self**

**vesr-1(config-security-zone-pair)# rule 3**

**vesr-1(config-security-zone-pair-rule)# description "TRACEROUTE"**

**vesr-1(config-security-zone-pair-rule)# action permit**

**vesr-1(config-security-zone-pair-rule)# match protocol udp**

**vesr-1(config-security-zone-pair-rule)# match destination-port TRACEROUTE**

**Syntax error: Illegal parameter**

**vesr-1(config-security-zone-pair-rule)# enable**

**vesr-1(config-security-zone-pair-rule)# exit**

**vesr-1(config-security-zone-pair)# exit**

**vesr-1(config)#**

Для зоны UNTRUST TRUST:

**vesr-1(config)# security zone-pair UNTRUST TRUST**

**vesr-1(config-security-zone-pair)# rule 2**

**vesr-1(config-security-zone-pair-rule)# action permit**

**vesr-1(config-security-zone-pair-rule)# match protocol udp**

**vesr-1(config-security-zone-pair-rule)# match destination-port object-group**

**TRACEROUTE**

**vesr-1(config-security-zone-pair-rule)# enable**

**vesr-1(config-security-zone-pair-rule)# exit**

**vesr-1(config-security-zone-pair)# exit**

**vesr-1(config)#**

Для зоны TRUST UNTRUST:

**vesr-1(config)# security zone-pair TRUST UNTRUST**

**vesr-1(config-security-zone-pair)# rule 2**

**vesr-1(config-security-zone-pair-rule)# action permit**

**vesr-1(config-security-zone-pair-rule)# match protocol udp**

**vesr-1(config-security-zone-pair-rule)# match destination-port object-group**

**TRACEROUTE**

**vesr-1(config-security-zone-pair-rule)# enable**

**vesr-1(config-security-zone-pair-rule)# exit**

**vesr-1(config-security-zone-pair)# exit**

**vesr-1(config)#**

Для удаленного филиала то же самое настраиваем:

Создается группа для сервиса traceroute:

**vesr-2# config**

**vesr-2(config)# object-group service TRACEROUTE**

**vesr-2(config-object-group-service)# port-range 33434-33534**

**vesr-2(config-object-group-service)# exit**

**vesr-2(config)# security zone-pair UNTRUST self**

**vesr-2(config-security-zone-pair)# rule 3**

**vesr-2(config-security-zone-pair-rule)# description "TRACEROUTE"**

**vesr-2(config-security-zone-pair-rule)# action permit**

**vesr-2(config-security-zone-pair-rule)# match protocol udp**

**vesr-2(config-security-zone-pair-rule)# enable**

**vesr-2(config-security-zone-pair-rule)# exit**

**vesr-2(config-security-zone-pair)# exit**

**vesr-2(config)**

И добавляем еще несколько правил в работу файвола:

Для зоны UNTRUST self

**vesr-2(config)# security zone-pair UNTRUST self**

**vesr-2(config-security-zone-pair)# rule 3**

**vesr-2(config-security-zone-pair-rule)# description "TRACEROUTE"**

**vesr-2(config-security-zone-pair-rule)# action permit**

**vesr-2(config-security-zone-pair-rule)# match protocol udp**

**vesr-2(config-security-zone-pair-rule)# match destination-port TRACEROUTE**

**Syntax error: Illegal parameter**

**vesr-2(config-security-zone-pair-rule)# enable**

**vesr-2(config-security-zone-pair-rule)# exit**

**vesr-2(config-security-zone-pair)# exit**

**vesr-2(config)#**

Для зоны UNTRUST TRUST:

**vesr-2(config)# security zone-pair UNTRUST TRUST**

**vesr-2(config-security-zone-pair)# rule 2**

**vesr-2(config-security-zone-pair-rule)# action permit**

**vesr-2(config-security-zone-pair-rule)# match protocol udp**

**vesr-2(config-security-zone-pair-rule)# match destination-port object-group**

**TRACEROUTE**

**vesr-2(config-security-zone-pair-rule)# enable**

**vesr-2(config-security-zone-pair-rule)# exit**

**vesr-2(config-security-zone-pair)# exit**

**vesr-2(config)#**

Для зоны TRUST UNTRUST:

**vesr-2(config)# security zone-pair TRUST UNTRUST**

**vesr-2(config-security-zone-pair)# rule 2**

**vesr-2(config-security-zone-pair-rule)# action permit**

**vesr-2(config-security-zone-pair-rule)# match protocol udp**

**vesr-2(config-security-zone-pair-rule)# match destination-port object-group**

**TRACEROUTE**

**vesr-2(config-security-zone-pair-rule)# enable**

**vesr-2(config-security-zone-pair-rule)# exit**

**vesr-2(config-security-zone-pair)# exit**

**vesr-2(config)#**

На каждом маршрутизаторе должен быть создан маршрут до локальной сети партнера. В качестве интерфейса назначения указываем ранее созданный туннель GRE:

На виртуальном роутере домашнего офиса маршрут до локальной сети удаленного офиса :

**vesr-1(config)# ip route 172.16.2.0/16 tunnel gre 10**

И на виртуальном роутере удаленного офиса зеркально маршрут до домашнего офиса:

**vesr-2(config)# ip route 172.16.1.0/16 tunnel gre 10**

Состояние туннеля можно посмотреть командой:

**vesr-1# sh tunnels configuration gre 10**

**State: Enabled**

**Description: --**

**Mode: ip**

**Bridge group: --**

**VRF: --**

**Local address: 10.10.10.2**

**Remote address: 10.10.20.2**

**Calculates checksums for outgoing GRE packets: No**

**Requires that all input GRE packets were checksum: No**

**key: --**

**TTL: 18**

**DSCP: Inherit**

**MTU: 1500**

**Path MTU discovery: Enabled**

**Don't fragment bit suppression: Disabled**

**Security zone: UNTRUST**

**Multipoint mode: Disabled**

**Keepalive:**

**State: Disabled**

**Timeout: 10**

**Retries: 6**

**Destination address: --**

**vesr-1#**

**vesr-2# sh tunnels configuration gre 20**

**State: Enabled**

**Description: --**

**Mode: ip**

**Bridge group: --**

**VRF: --**

**Local address: 10.10.20.2**

**Remote address: 10.10.10.2**

**Calculates checksums for outgoing GRE packets: No**

**Requires that all input GRE packets were checksum: No**

**key: --**

**TTL: 18**

**DSCP: Inherit**

**MTU: 1500**

**Path MTU discovery: Enabled**

**Don't fragment bit suppression: Disabled**

**Security zone: UNTRUST**

**Multipoint mode: Disabled**

**Keepalive:**

**State: Disabled**

**Timeout: 10**

**Retries: 6**

**Destination address: --**

**vesr-2#**

Счетчики входящих и отправленных пакетов можно посмотреть командой:

**vesr-1# show tunnels counters gre 10**

Конфигурацию туннеля можно посмотреть командой:

**vesr-1# show tunnels configuration gre 10**

Настройка туннеля для удаленного филиала производится аналогичным образом.

После применения настроек трафик будет инкапсулироваться в туннель и отправляться партеру, независимо от наличия GRE-туннеля и правильности настроек с его стороны.

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)**

Теперь все работает как надо.

Настройка IPSEC:

Создадим профиль протокола IKE. В профиле укажем группу Диффи-Хэллмана 2, алгоритм шифрования AES 128 bit, алгоритм аутентификации MD5. Данные параметры безопасности используются для защиты IKE-соединения:

vESR-1 | vESR-2

Copy

security ike proposal ike\_prop1

authentication algorithm md5

encryption algorithm aes128

dh-group 2

exit

7. Создадим политику протокола IKE. В политике указывается список профилей протокола IKE, по которым могут согласовываться узлы и ключ аутентификации:

vESR-1 | vESR-2

Copy

security ike policy ike\_pol1

pre-shared-key ascii-text P@ssw0rd

proposal ike\_prop1

exit

8. Создадим шлюз протокола IKE. В данном профиле указывается GRE-туннель, политика, версия протокола и режим перенаправления трафика в туннель:

vESR-1

Copy

security ike gateway ike\_gw1

ike-policy ike\_pol1

local address 1.1.1.2

local network 1.1.1.2/32 protocol gre

remote address 2.2.2.2

remote network 2.2.2.2/32 protocol gre

mode policy-based

exit

vESR-2

Copy

security ike gateway ike\_gw1

ike-policy ike\_pol1

local address 2.2.2.2

local network 2.2.2.2/32 protocol gre

remote address 1.1.1.2

remote network 1.1.1.2/32 protocol gre

mode policy-based

exit

9. Создадим профиль параметров безопасности для IPsec-туннеля. В профиле укажем группу Диффи-Хэллмана 2, алгоритм шифрования AES 128 bit, алгоритм аутентификации MD5. Данные параметры безопасности используются для защиты IPsec-туннеля:

vESR-1 | vESR-2

Copy

security ipsec proposal ipsec\_prop1

authentication algorithm md5

encryption algorithm aes128

pfs dh-group 2

exit

10. Создадим политику для IPsec-туннеля. В политике указывается список профилей IPsec-туннеля, по которым могут согласовываться узлы.

vESR-1 | vESR-2

Copy

security ipsec policy ipsec\_pol1

proposal ipsec\_prop1

exit

11. Создадим IPsec VPN. В VPN указывается шлюз IKE-протокола, политика IP sec-туннеля, режим обмена ключами и способ установления соединения. После ввода всех параметров включим туннель командой enable.

vESR-1 | vESR-2

Copy

security ipsec vpn ipsec1

ike establish-tunnel route

ike gateway ike\_gw1

ike ipsec-policy ipsec\_pol1

enable

exit

12. Настраиваем firewall:

vESR-1 | vESR-2

Copy

security zone-pair WAN self

rule 2

description "GRE"

action permit

match protocol gre

enable

exit

rule 3

description "ESP"

action permit

match protocol esp

enable

exit

rule 4

description "AH"

action permit

match protocol ah

enable

exit

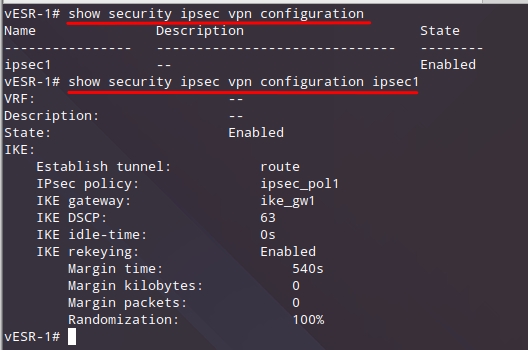
exit

Copy

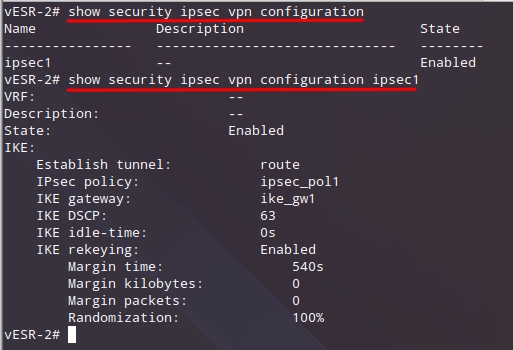
do commit

do confirm

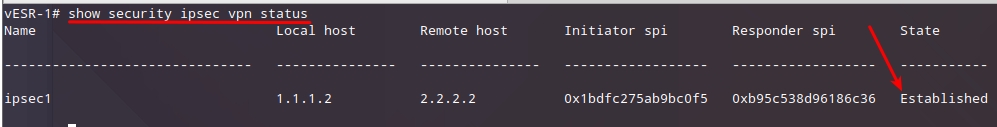
Проверяем:



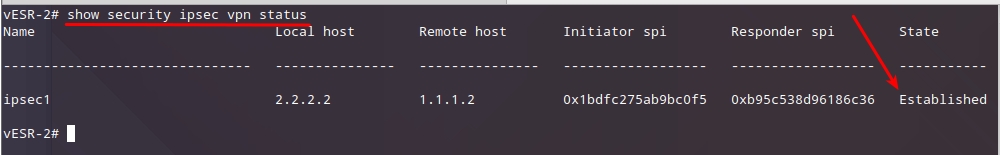
img



img

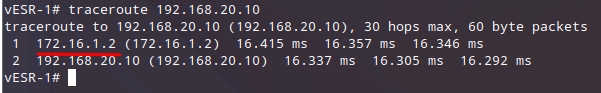


img

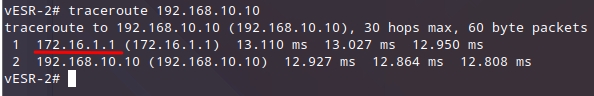


img

* **traceroute** - работает только после разрешения в firewall
  + можно посмотреть в ниже в полной конфигурации устройств;



img



img