**Глава 8. Настройка Destination NAT на виртуальном маршрутизаторе vesr**

**Немного теории, без которой , как всем известно древо не зеленеет ( шутка)-DNAT (Destination Network Address Translation)** — это тип технологии NAT (Network Address Translation), которая **изменяет адрес и порт назначения входящего пакета**.  [newstorial.com](https://www.newstorial.com/what-is-dnat/)[expertnetworkconsultant.com](https://www.expertnetworkconsultant.com/expert-approach-in-successfully-networking-devices/navigating-network-address-translation-understanding-the-difference-between-dnat-and-snat/)[docs.selectel.ru](https://docs.selectel.ru/vmware/public-cloud/manage-networks/nat-rules/)

**Механизм работы** DNAT включает три этапа:  [newstorial.com](https://www.newstorial.com/what-is-dnat/)

1. **Анализ входящего пакета**. Устройство (маршрутизатор или файрвол) проверяет адрес назначения и номер порта.  [newstorial.com](https://www.newstorial.com/what-is-dnat/)
2. **Преобразование**. На основе заранее определённых правил маршрутизатор или файрвол заменяет адрес назначения и, возможно, номер порта.  [newstorial.com](https://www.newstorial.com/what-is-dnat/)
3. **Направление пакета**. После преобразования пакет отправляется к новому адресу внутри частной сети.  [newstorial.com](https://www.newstorial.com/what-is-dnat/)

DNAT используется в различных сценариях, например:

* **Балансировка нагрузки**. Входящие запросы распределяются между несколькими серверами, чтобы эффективно использовать ресурсы и избежать перегрузки одного сервера.  [newstorial.com](https://www.newstorial.com/what-is-dnat/)
* **Перенаправление портов**. Позволяет внешним устройствам получать доступ к сервисам в частной сети, сопоставляя внешний порт с внутренним IP-адресом и портом.  [newstorial.com](https://www.newstorial.com/what-is-dnat/" \t "_blank)[docs.ideco.dev](https://docs.ideco.dev/settings/access-rules/firewall/firewall-tables)
* **Настройка виртуальных частных сетей (VPN)**. DNAT перенаправляет трафик из публичной сети в частную, что помогает обеспечить безопасность соединения.  [newstorial.com](https://www.newstorial.com/what-is-dnat/)

Предположим, что нужно еще один малый офис подключить в сеть Интернет и обеспечить доступ из нее к серверу SSH в домашнем офисе. Доступ будет из сети относящейся к зоне «UNTRUST» виртуального маршрутизатора, к серверу SSH в домашней локальной сети в зоне «TRUST». Адрес сервера в локальной сети – 172.16.1.3 ( адрес интерфейса Eth0 виртуальной машины MicroCoreLinux6.4-1 ). Сервер должен быть доступным извне по адресу 10.10.10.2 (адрес интерфейса Gi1/0/1 виртуального маршрутизатора vesr-1) , доступный порт 2222.

Имитацию публичной сети можно организовать через дополнительный виртуальный маршрутизатор с именем vesr-3 и еще одну локальную сеть в виде дубля схемы на Рис.

Каждый новый виртуальный маршрутизатор на схеме требует отдельной первоначальной инициации , как описано главе 2. «Настройка виртуального сервисного маршрутизатора vESR для работы в среде виртуализации GNS3» и в главе 4 «Базовая настройка vESR».

Сначала настраиваем в самом простом варианте центральный виртуальный маршрутизатор vesr-3 и затем виртуальный маршрутизатор домашнего офиса vesr-1.

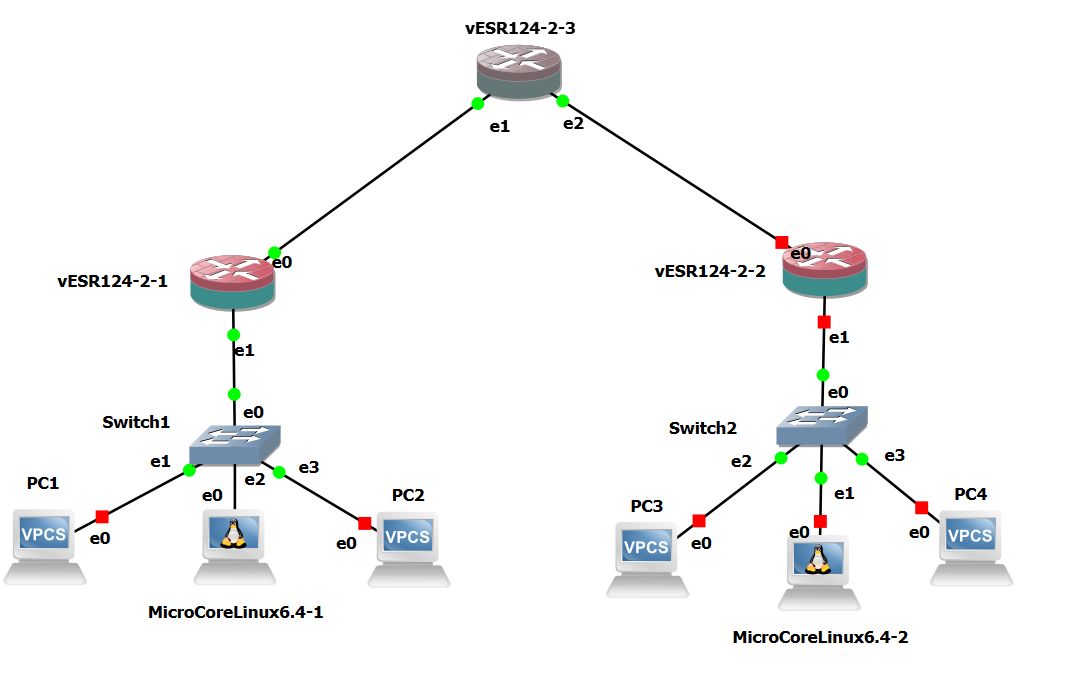


Рис.

Настройка центрального виртуального маршрутизатора vesr:

Дадим ему название, выключим мжсетевой экран и назначим IP адрес на интерфейсе gi1/0/1:

**vesr(config)# hostname vesr-Odin**

**vesr(config)# exit**

**vesr(config)# do commit**

**vesr(config)# do confirm**

**vesr-Odin(config)# int gigabitethernet 1/0/1**

**vesr-Odin(config-if-gi)# description "link2vesr-2"**

**vesr-Odin(config-if-gi)# ip firewall disable**

**vesr-Odin(config-if-gi)# ip address 10.10.10.1/24**

**vesr-Odin(config-if-gi)# exit**

**vesr(config)# do commit**

**vesr(config)# do confirm**

так же настроим второй интерфейс:

**vesr-Odin(config)# int gigabitethernet 1/0/2**

**vesr-Odin(config-if-gi)# description "link2vesr-3"**

**vesr-Odin(config-if-gi)# ip firewall disable**

**vesr-Odin(config-if-gi)# ip address 10.10.20.1/24**

**vesr-Odin(config-if-gi)# exit**

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

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

Включим маршрутизацию :

**vesr-Odin(config)#** ip route 10.10.10.0/24 interface gigabitethernet 1/0/2

**vesr-Odin(config)#** ip route 10.10.20.0/24 interface gigabitethernet 1/0/3

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

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

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

**vesr-Odin(config)# exit**

От центрального маршрутизатора понадобится только простая маршрутизация пакетов IP. Поэтому мэжсетевой экран на обоих интерфейсах отключен.

На этом настройка центрального виртального маршрутизатора завершена.

Настройка виртуального маршрутизатора vesr-1 (он использовался и в предыдущих работах в этом руководстве, но здесь есть небольшие изменения):

Создадим зоны безопасности «UNTRUST» и «TRUST». Установим принадлежность используемых сетевых интерфейсов к зонам. Одновременно назначим IP-адреса интерфейсам.

**vesr-1# configure  
vesr-1(config)# security zone UNTRUST  
vesr-1(config-zone)# exit  
vesr-1(config)# security zone TRUST  
vesr-1(config-zone)# exit  
vesr-1(config)# interface gigabitethernet 1/0/1  
vesr-1(config-if-gi)# security-zone UNTRUST  
vesr-1(config-if-gi)# ip address 10.10.10.1/24  
vesr-1(config-if-gi)# exit  
vesr-1(config)# interface gigabitethernet 1/0/2  
vesr-1(config-if-te)# ip address 172.16.1.1/24  
vesr-1(config-if-te)# security-zone TRUST  
vesr-1(config-if-te)# exit**

Создадим профили IP-адресов и портов, которые потребуются для настройки правил Firewall и правил DNAT.

* WAN – профиль адресов публичной сети;
* LAN\_NATWORK – профиль адресов локальной сети;
* SSH – профиль портов.
* SERVER\_IP – профиль адреса сервера ssh.

**vesr-1(config)# object-group network WAN  
vesr-1(config-object-group-network)# ip address 10.10.10.2  
vesr-1(config-object-group-network)# exit  
vesr-1(config)# object-group service SSH  
vesr-1(config-object-group-network)# port-range 2222  
vesr-1(config-object-group-network)# exit  
vesr-1(config)# object-group network SERVER\_IP  
vesr-1(config-object-group-network)# ip address 172.16.1.3  
vesr-1(config-object-group-network)# exit**

Войдем в режим конфигурирования функции DNAT и создадим пул адресов и портов назначения, в которые будут транслироваться адреса пакетов, поступающие на адрес 10.10.10.2 из внешней сети.

**vesr-1(config)# nat destination  
vesr-1(config-dnat)# pool SERVER\_POOL  
vesr-1(config-dnat-pool)# ip address 172.16.1.3  
vesr-1(config-dnat-pool)# ip port 22  
vesr-1(config-dnat-pool)# exit**

Создадим набор правил «DNAT», в соответствии с которыми будет производиться трансляция адресов. В атрибутах набора укажем, что правила применяются только для пакетов, пришедших из зоны «UNTRUST». Набор правил включает в себя требования соответствия данных по адресу и порту назначения (match destination-address, match destination-port) и по протоколу. Кроме этого в наборе задано действие, применяемое к данным, удовлетворяющим всем правилам (action destination-nat). Набор правил вводится в действие командой «enable».

**vesr-1(config-dnat)# ruleset DNAT  
vesr-1(config-dnat-ruleset)# from zone UNTRUST  
vesr-1(config-dnat-ruleset)# rule 1  
esr(config-dnat-rule)# match destination-address object-group WAN  
esr(config-dnat-rule)# match protocol tcp  
esr(config-dnat-rule)# match destination-port object-group SSH  
esr(config-dnat-rule)# action destination-nat pool SERVER\_POOL  
esr(config-dnat-rule)# enable  
esr(config-dnat-rule)# exit  
esr(config-dnat-ruleset)# exit  
esr(config-dnat)# exit**

Для пропуска трафика, идущего из зоны «UNTRUST» в «TRUST», создадим соответствующую пару зон. Пропускать следует только трафик с адресом назначения, соответствующим заданному в профиле «SERVER\_IP», и прошедший преобразование DNAT.

**vesr-1(config)# security zone-pair UNTRUST TRUST  
vesr-1(config-zone-pair)# rule 1  
vesr-1(config-zone-rule)# match source-address any  
vesr-1(config-zone-rule)# match destination-address objct-group SERVER\_IP  
vesr-1(config-zone-rule)# match protocol any  
vesr-1(config-zone-rule)# match destination-nat  
vesr-1(config-zone-rule)# action permit  
vesr-1(config-zone-rule)# enable  
vesr-1(config-zone-rule)# exit  
vesr-1(config-zone-pair)# exit  
vesr-1(config)# exit**

Изменения конфигурации вступят в действие после применения:

**vesr-1# commit  
Configuration has been successfully committed  
esr# confirm  
Configuration has been successfully confirmed**

Произведенные настройки можно посмотреть с помощью команд:

**vesr-1# show ip nat destination pools  
vesr-1# show ip nat destination rulesets  
vesr-1# show ip nat proxy-arp  
vesr-1# show ip nat translations**

Поверяем доступ к серверу SSH на виртуальной машине MicroCoreLinux6.4-1 непосредственно с виртуального маршрутизатора vesr-3, поскольку он находится в зоне UNTRUST и может имитировать доступ извне:

**vesr-Odin# ssh gns3 10.10.10.2 port 2222**

**gns3@10.10.10.2's password:gns3**

**( '>')**

**/) TC (\ Core is distributed with ABSOLUTELY NO WARRANTY.**

**(/-\_--\_-\)** [**www.tinycorelinux.net**](http://www.tinycorelinux.net)

**gns3@box:~$ pwd**

**/home/gns3**

**gns3@box:~$ ls -al**

**total 12**

**drwxr-sr-x 3 gns3 staff 120 Jun 11 09:16 ./**

**drwxrwxr-x 3 root staff 60 Oct 8 2015 ../**

**-rw-rw-r-- 1 gns3 staff 321 Jun 11 09:39 .ash\_history**

**-rw-r--r-- 1 gns3 staff 446 Oct 8 2015 .ashrc**

**drwxr-sr-x 3 gns3 staff 60 Jun 11 09:16 .local/**

**-rw-r--r-- 1 gns3 staff 920 Oct 8 2015 .profile**

**gns3@box:~$**

Проверяем настройки и трансляцию:

**vesr-1# sh ip nat translations**

**Prot Inside source Inside destination Outside source Outside destination Pkts Bytes**

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

**icmp 172.16.1.3 10.10.20.1 10.10.10.2 10.10.20.1 -- --**

**vesr-1# sh ip nat translations**

**Prot Inside source Inside destination Outside source Outside destination Pkts Bytes**

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

**tcp 10.10.10.1:38358 172.16.1.3:22 10.10.10.1:38358 10.10.10.2:2222 -- --**

**icmp 172.16.1.3 10.10.20.1 10.10.10.2 10.10.20.1 -- --**

**icmp 172.16.1.3 1.1.1.1 10.10.10.2 1.1.1.1 -- --**

**udp 172.16.1.3:43522 77.88.8.8:53 10.10.10.2:43522 77.88.8.8:53 -- --**

**vesr-1# sh ip nat destination pools**

**Name IP Port Description**

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

**SERVER\_POOL 172.16.1.3 22 --**

**vesr-1# sh ip nat destination rulesets**

**Name From Description**

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

**DNAT zone 'UNTRUST' --**

**vesr-1#**

DNAT на виртуальном маршрутизаторе vesr-1 и маршрутизация на vesr-Odin работают.

Как всем известно есть поговорка-«Повторение-мать учения», поэтому для закрепления повторим шаги описанные в предыдущих главах применив их к новому малому офису.

Переходим к настройке удаленного офиса с виртуальным маршрутизатором vesr-2. Схема подключения аналогичная той, что была описана выше применительно к сети домашнего офиса. Подключена эта сеть к интерфейсу gi1/0/2 виртуального маршрутизатора vesr-Odin с IP адресом 10.10.20.1. Следовательно, назначим IP адрес 10.10.20.2 интерфейсу Gi1/0/1 виртуального маршрутизатора vesr-2 не забыв создать зоны контроля:

**vesr-2#config**

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

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

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

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

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

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

**vesr-2(config)# int gigabitethernet 1/0/1**

**vesr-2(config-if-gi)# description UPLINK**

**vesr-2(config-if-gi)# ip address 10.10.20.2/24**

**vesr-2(config-if-gi)# security-zone UNTRUST**

**vesr-2(config-if-gi)# exit**

**vesr-2(config)# int gigabitethernet 1/0/2**

**vesr-2(config-if-gi)# description LAN2**

**vesr-2(config-if-gi)# ip address 172.16.2.1/24**

**vesr-2(config-if-gi)# security-zone TRUST**

**vesr-2(config-if-gi)# exit**

**vesr-2#config**

Сохраняем конфиг и проверяем результат:

**vesr-2(config)# do commit**

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

**2025-06-11T10:09:31+00:00 %CLI-I-CRIT: user admin from console input: do commit**

**vesr-2(config)# do confirm**

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

**2025-06-11T10:09:34+00:00 %CLI-I-CRIT: user admin from console input: do confirm**

**vesr-2(config)# do sh run security zone**

**security zone UNTRUST**

**exit**

**security zone TRUST**

**exit**

**interface gigabitethernet 1/0/1**

**security-zone UNTRUST**

**exit**

**interface gigabitethernet 1/0/2**

**security-zone TRUST**

**exit**

**vesr-2(config)# do 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**

**vesr-2(config)#**

Локальная сеть малого офиса состоит из трех устройств – эмуляторов ПК PC3, PC4 и виртуальной машины с Линукс – MicroCoreLinux6.4-2. Сделаем на виртуальном маршрутизаторе vesr-2 сервер DHCP для получения ими IP адресов автоматически:

**vesr-2(config)# ip dhcp-server pool LAN2**

**vesr-2(config-dhcp-server)# network 172.16.2.0/24**

**vesr-2(config-dhcp-server)# default-lease-time 3:00:00**

**vesr-2(config-dhcp-server)# address-range 172.16.2.1-172.16.2.254**

**vesr-2(config-dhcp-server)# excluded-address-range 172.16.2.1**

**vesr-2(config-dhcp-server)# excluded-address-range 172.16.2.254**

**vesr-2(config-dhcp-server)# default-router 172.16.2.1**

**vesr-2(config-dhcp-server)# dns-server 77.88.8.8**

**vesr-2(config-dhcp-server)# exit**

**vesr-2(config)# do commit**

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

**2025-06-11T10:29:59+00:00 %CLI-I-CRIT: user admin from console input: do commit**

**vesr-2(config)# doconfirm**

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

**2025-06-11T10:30:02+00:00 %CLI-I-CRIT: user admin from console input: do confirm**

**vesr-2(config)#**

В приведенном списке команда создается пул сервера DHCP с названием LAN2, резервируется сеть 172.16.2.0/24 класса С, ограничивается время аренды адресов тремя часами, выделяется диапазон арендуемых адресов из этой сети, исключаются из диапазона первый и последний адреса. Назначается адрес роутера по умолчанию и адрес сервера DNS.

Для разрешения прохождения сообщений протокола DHCP к серверу необходимо создать соответствующие профили портов, включающие порт источника 68 и порт назначения 67, используемые протоколом DHCP, и создать разрешающее правило в политике безопасности для прохождения пакетов протокола UDP используем набор команд :

**vesr-2(config)# object-group service dhcp\_service**

**vesr-2(config-object-group-service)# port-range 68**

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

**vesr-2(config)# object-group service dhcp\_client**

**vesr-2(config-object-group-service)# port-range 68**

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

Для настройки пропуска пакетов из одной зоны в другую нужно описать сетевые и сервисные объекты. Сервисные были описаны выше. Создаем сетевые объекты:

**vesr-2(config)# object-group network GATEWAY\_TO\_LAN**

**vesr-2(config-object-group-network)# ip address-range 172.16.2.1**

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

**vesr-2(config)# object-group network LAN\_NETWORK**

**vesr-2(config-object-group-network)# ip address-range 172.16.2.1-172.16.2.254**

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

**vesr-2(config)# object-group network WAN**

**vesr-2(config-object-group-network)# ip address-range 10.10.20.1**

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

Здесь объект с именем GATEWAY\_TO\_LAN описывает адрес дефолтного роутера для устройств в локальной сети. Объект LAN\_NETWORK описывает диапазон адресов локальной сети, а объект WAN описывает адрес выходного интерфейса в публичную сеть Интернет.

Для работы протокола DHCP необходимо разрешить прохождение пакетов через зону TRUST к самому маршрутизатору:

Для контроля связности устройств в локальной сети с виртуальным маршрутизатором необходимо так же разрешить прохождение пакетов ICMP через доверенную зону:

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

**vesr-2(config-security-zone-pair)# rule 9**

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

**vesr-2(config-security-zone-pair-rule)# match destination-address object-group LAN\_NETWORK**

**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)# ip dhcp-server**

**vesr-2(config)# do commit**

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

**2025-06-11T14:04:15+00:00 %CLI-I-CRIT: user admin from console input: do commit**

**vesr-2(config)# do confirm**

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

**2025-06-11T14:04:19+00:00 %CLI-I-CRIT: user admin from console input: do confirm**

**vesr-2(config)# exit**

**vesr-2#**

Проверяем назначение адреса и доступность роутера с ПК PC3:

**PC3> ip dhcp**

**DORA IP 172.16.2.3/24 GW 172.16.2.1**

**PC3> ping 172.16.2.1**

**84 bytes from 172.16.2.1 icmp\_seq=1 ttl=64 time=3.233 ms**

**84 bytes from 172.16.2.1 icmp\_seq=2 ttl=64 time=3.877 ms**

**84 bytes from 172.16.2.1 icmp\_seq=3 ttl=64 time=2.088 ms**

**84 bytes from 172.16.2.1 icmp\_seq=4 ttl=64 time=3.946 ms**

**84 bytes from 172.16.2.1 icmp\_seq=5 ttl=64 time=2.750 ms**

**PC3> save PC3**

**Saving startup configuration to PC3.vpc**

**. done**

Адреса раздаются и связность сети с роутером есть. Переходим к настройки SNAT ( что это такое описано в главе 6 «Настройка NAT(SNAT) для доступа в Интернет в маршрутизаторе vESR», поэтому повторим с небольшими изменениями материал этой главы для настройки трансляции IP пакетов в публичную сеть Интернет с заменой исходящего адреса на внешний. Проверяем связность локально сети малого офиса с внешним миром:

**gns3@box:~$ ip add | grep eth0**

**5: eth0: <BROADCAST,MULTICAST,UP,LOWER\_UP> mtu 1500 qdisc pfifo\_fast state UP qlen 1000**

**inet 172.16.2.2/24 brd 172.16.2.255 scope global eth0**

**gns3@box:~$ ping 77.88.8.8**

**PING 77.88.8.8 (77.88.8.8): 56 data bytes**

**^C**

**--- 77.88.8.8 ping statistics ---**

**4 packets transmitted, 0 packets received, 100% packet loss**

**gns3@box:~$**

Пакеты IP не ходят.

Настраиваем SNAT. Для пропуска трафика из зоны **trusted** в зону **untrusted** создадим пару зон и добавим правила, разрешающие проходить трафику в этом направлении. Дополнительно включена проверка адреса источника данных на принадлежность к диапазону адресов LAN\_NETWORK для соблюдения ограничения на выход в публичную сеть. Действие правил разрешается командой enable:

**vesr-2#config**

**vesr-2(config)#**

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

**vesr-2(config-security-zone-pair)# rule 10**

**vesr-2(config-security-zone-pair-rule)# match source-address object-group LAN\_NETWORK**

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

**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)# do commit**

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

**2025-06-11T14:28:44+00:00 %CLI-I-CRIT: user admin from console input: do commit**

**vesr-2(config)# do confirm**

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

**2025-06-11T14:28:50+00:00 %CLI-I-CRIT: user admin from console input: do confirm**

**vesr-2(config)#**

Источник документации к командам к виртуальному маршрутизатору:

docs.eltex-co.ru