

Ринат Х. Фахрутдинов

РУКОВОДСТВО ДЛЯ РАБОТЫ С
МАРШРУТИЗАТОРОМ VESR
В СИМУЛЯТОРЕ GNS3

книга 1



Москва

2025 г.

1. Оглавление

.....	1
ВВЕДЕНИЕ	4
Глава 1. Создание образа виртуального маршрутизатора vESR Eltex для работы в среде виртуализации GNS3.....	7
Выводы по главе	30
Глава 2. Почему GNS3, а не EVE-NG?	32
Выводы по главе	32
Глава 3. Базовая настройка виртуального маршрутизаторе vESR.....	33
Выводы по главе	57
Глава 4. Настройка сервера DHCP в маршрутизаторе vESR.....	58
Выводы по главе	67
Глава 5. Настройка NAT(SNAT) для доступа в Интернет в виртуальном маршрутизаторе vESR.....	69
Выводы по главе	76
Глава 6. Настройка SSH в виртуальном маршрутизаторе vESR....	77
Выводы по главе	93
Глава 7. Настройка NAT(DNAT) для доступа в Интернет в виртуальном маршрутизаторе vESR.....	94
Выводы по главе	110
Глава 8. Настройка GRE-over-IPSEC в маршрутизаторе vESR....	111
Выводы по главе	148
Глава 9. Настройка нескольких филиалов с на виртуальных маршрутизаторах vESR.	150
Выводы по главе	169
Глава 10. Настройка динамической (OSPF) маршрутизации в виртуальном маршрутизаторе vESR.....	170
Выводы по главе	209
Список литературы.....	213
Приложение.....	214

Об авторе

Системный и сетевой инженер с более чем 40 летним стажем. Начинал карьеру в информационных технологиях в конце 70-х годов прошлого века на советских еще транзисторных мейнфреймах ЭВМ "Минск-32" программистом на языке программирования Кобол, затем была эпоха машин серии ЕС ЭВМ и языков Фортран, PL/I и Паскаль, конец 80-х годов 20 века отмечен интересными машинами серии СМ-4 и СУБД Адабас-М. В 90-е осваивал первым персоналки фирмы IBM и программирование баз данных FoxBase. Тогда же и освоил построение первых локальных сетей для предприятия уровня большого горно-обогатительного комбината на Севере. Конец века застал меня сотрудником Курчатовского института в одном из первых интернет сервис провайдеров страны - Релком. С тех пор моя работа неразрывно связана с сетями передачи данных, с сетевым оборудованием и операционными системами для них. Работаю с ОС Unix/Linux разных типов, Windows с самых первых выпусков. Сейчас изучаю оборудование отечественного производителя. Для обучающихся работе с ним написал две книги.

ВВЕДЕНИЕ

Прежде чем мы погрузимся в мир туннельных технологий, разрешите выразить искреннюю благодарность всем, кто приобрел электронную версию этой книги. Ваша поддержка не просто вдохновляет — она позволяет развивать проект дальше, делая сложные сетевые концепции доступнее для сообщества.

Особые слова признательности:

- **Читателям** первых версий за ценные правки,
- **Коллегам** за практические кейсы,
- **Всем**, кто верит, что знания должны быть живыми и прикладными.

Эта книга — наш общий труд. Если в процессе изучения у вас возникнут вопросы, идеи или замечания, буду рад диалогу!

Теперь — к делу!

Современные сетевые технологии требуют не только теоретических знаний, но и практических навыков работы с оборудованием. Однако доступ к реальным маршрутизаторам и коммутаторам зачастую ограничен, особенно на этапе обучения. Выходом становится использование виртуальных сред, таких как **GNS3**, которые позволяют моделировать сложные сети на обычном компьютере.

Эта книга для новичков в сетевых технологиях и посвящена работе с виртуальным сервисным маршрутизатором vESR от Eltex. vESR. На сайте производителя <https://eltex-co.ru/catalog/virtualnyi-servisnyi-marsrutizator-vesr> приводится такая характеристика этого маршрутизатора— «программный аналог аппаратных сервисных маршрутизаторов Eltex серии ESR, предоставляющий те же возможности, но с гибкостью внедрения и использования в виртуальных средах. Виртуальный маршрутизатор может применяться: в корпоративных сетях любого размера, гибридных инфраструктурах, лабораториях в составе тестовых стендов при разработке новых сервисов. Используется как самостоятельное решение или дополнение к физической инфраструктуре, например для резервирования основного шлюза и балансировки нагрузки. Эффективно решает задачи, связанные с обработкой трафика и безопасностью сети. Поддерживаются: расширенные функции L2 и L3, VPN, VLAN, QoS, MPLS, NAT, межсетевой экран и др. Запускается на Linux-сервере на популярных популярных гипервизорах Xen, Oracle VirtualBox, VMware ESXI. Поддерживается расширенный набор функций L3. Среди них:

Статическая маршрутизация

Динамическая маршрутизация (IPv4/IPv6): OSPFv2/v3, IS-IS, BGP, RIPv2, RIP

MPLS: LDP, L2VPN, L3VPN, MPLS over GRE

Трансляция сетевых адресов: ALG, Static NAT и NAT

VRF, PBR и др.».

Начнем с базовых шагов: установки GNS3, создания образа vESR и его первоначальной настройки. Далее вы освоите ключевые аспекты работы маршрутизатора, от настройки SSH до организации защищённых туннелей GRE-over-IPSec для сети офиса с филиалами.

Для кого эта книга?

Сетевые администраторы, желающие освоить vESR.

Студенты и преподаватели, изучающие маршрутизацию и виртуализацию.

Подготовка к сертификациям: лабораторные работы помогут закрепить теорию на практике.

Структура книги

Каждая глава содержит:

- Пошаговые инструкции с скриншотами (где это необходимо).
- Примеры конфигураций и их разбор.
- Советы по диагностике и устранению типовых ошибок.
- Что потребуется?
- GNS3 (желательно версии 2.2.52 или новее).
- Образ vESR (например, версии 1.24-2).
- VMware Workstation.
- Terminal-клиенты (PuTTY, UltraVNC).

Важно! Даже если вы новичок в GNS3 или vESR, книга поможет вам начать — от создания первой виртуальной сети до сложных сценариев маршрутизации. Готовы? Тогда вперёд — к первой главе!

Об авторе

Системный и сетевой инженер с более чем 40 летним стажем. Начинал карьеру в информационных технологиях в конце 70-х годов прошлого века на советских еще транзисторных мейнфреймах ЭВМ "Минск-32" программистом на языке программирования Кобол, затем была эпоха машин серии ЕС ЭВМ и языков Фортран, PL/I и Паскаль, конец 80-х годов 20 века отмечен интересными машинами серии СМ-4 и СУБД Адабас-М. В 90-е осваивал первым персоналки фирмы IBM и программирование баз данных FoxBase. Тогда же и освоил построение первых локальных сетей для предприятия уровня большого горно-обогатительного комбината на Севере. Конец века застал меня сотрудником курчатовского института в одном из первых интернет сервис провайдеров страны - Релком. С тех пор моя работа неразрывно связана с сетями передачи данных, с сетевым оборудованием и операционными системами для них. Работаю с ОС Unix/Linux разных типов, Windows с самых первых выпусков. Сейчас изучаю оборудование отечественного производителя. Для обучающихся работе с ним написал книгу.

Глава 1. Создание образа виртуального маршрутизатора vESR Eltex для работы в среде виртуализации GNS3.

Цель этой работы:

Установить необходимое программное обеспечение для прохождения всех лабораторных работ.

Установку программы GNS3 (Graphical Network Simulator 3), которая представляет собой мощный программный комплекс для моделирования и тренировки сетевых администраторов лучше всего посмотреть и почитать на оригинальном ресурсе <https://docs.gns3.com/docs/getting-started/installation/windows/>.

Загрузить последнюю версию можно по адресу <https://github.com/GNS3/gns3-gui/releases>.

В этой главе описан процесс создания и добавления загрузочного образа для виртуального маршрутизатора vESR Eltex версии 1.24-2 в программе GNS3 для новичков впервые знакомящихся с возможностями как симулятора, так и виртуального маршрутизатора vESR.

Кроме этого понадобится дополнительный набор программного обеспечения:

- программа UltraVNC (иногда пишется как uVNC) — это свободное программное обеспечение для операционной системы Microsoft Windows, которое использует протокол VNC для управления удалёнными рабочими столами на других компьютерах., взять и настроить её можно здесь - <https://uvnc.com/docs/ultravnc-server/49-ultravnc-server-configuration.html>
- программа PuTTY — клиентская программа для работы с сетевыми протоколами Telnet, SSH, SCP, SFTP, для подключения по COM-порту и ZModem, утилита для генерации RSA, DSA, ECDSA, Ed25519 цифровых SSH-ключей, является свободным приложением с открытым исходным кодом. Загрузить можно с сайта <https://putty.org.ru/download>
- VMware Workstation — программное обеспечение виртуализации, предназначенное для компьютеров с операционными системами Microsoft Windows и Linux. Позволяет пользователю установить одну или более виртуальных машин на один физический компьютер и запускать их параллельно с ним. Официальная документация находится по адресу

Лабораторные работы с виртуальным сервисным маршрутизатором vESR
В графическом симуляторе GNS3

<https://techdocs.broadcom.com/us/en/vmware-cis/desktop-hypervisors/workstation-pro/17-0/using-vmware-workstation-pro.html>. Для загрузки дистрибутива нужна регистрация на сайте <https://www.vmware.com/products/desktop-hypervisor/workstation-and-fusion>.

В процессе установки программы GNS3 будет предложен выбор установки виртуальной машины GNS3, рекомендуется для скачивания образ VMware VM. Установка программы виртуализации VMware Workstation описана, например, по адресу <https://ultahost.com/knowledge-base/install-vmware-on-windows/>. После его установки и старта в дальнейшем этой виртуальной машины для поиска возможных ошибок с сетью нужно проверить настройки этой машины. В частности, запустить главное окно программы VMware Workstation Pro и посмотреть вот на эти экраны и установить доступ виртуальной машины к основному хостовому ПК через NAT:

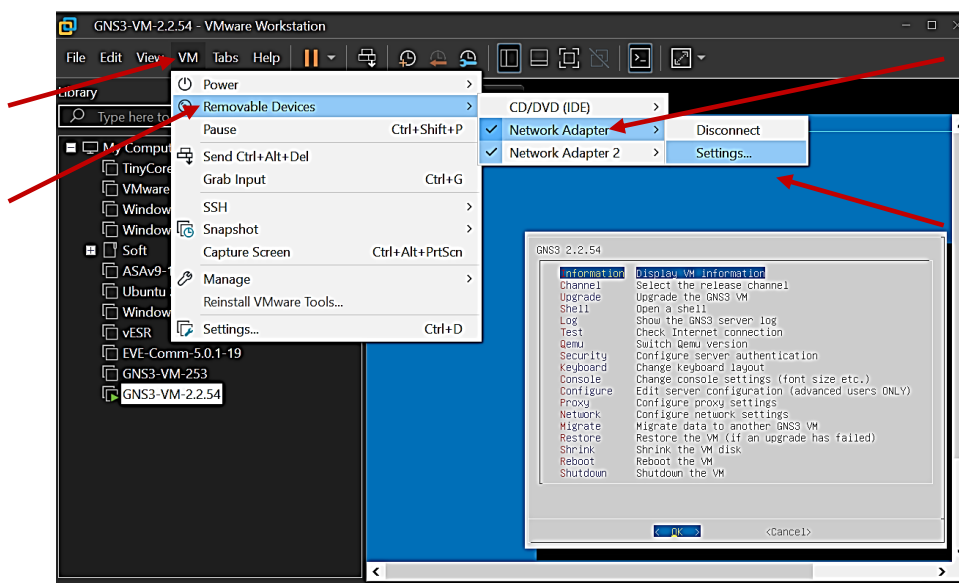


Рисунок 1-1. Изображение главного экрана программы VMware Workstation — программное обеспечение виртуализации, предназначенное для компьютеров x86-64 операционных систем Microsoft Windows и Linux.

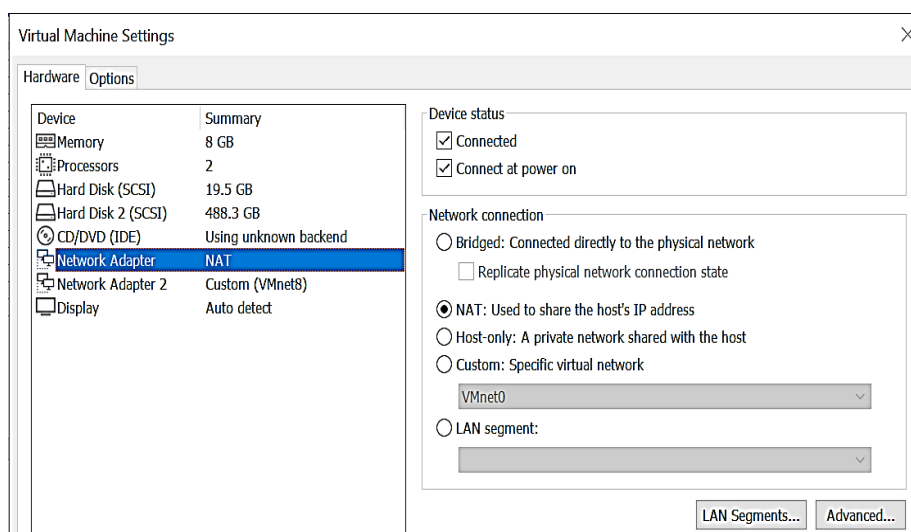


Рисунок 1-2 Выбор режима сети – NAT при подключении виртуальной машины GNS3 в программе VMware Workstation Pro.

Затем по нажатию на пункт ОК зафиксировать выбор. Консоль терминала работает через программы VNC или Putty. Putty свободно распространяемая программа доступна по адресу <https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html>.

В начале, сразу после старта программы GNS3 нужно перейти в свойства программы Edit->Preferences:

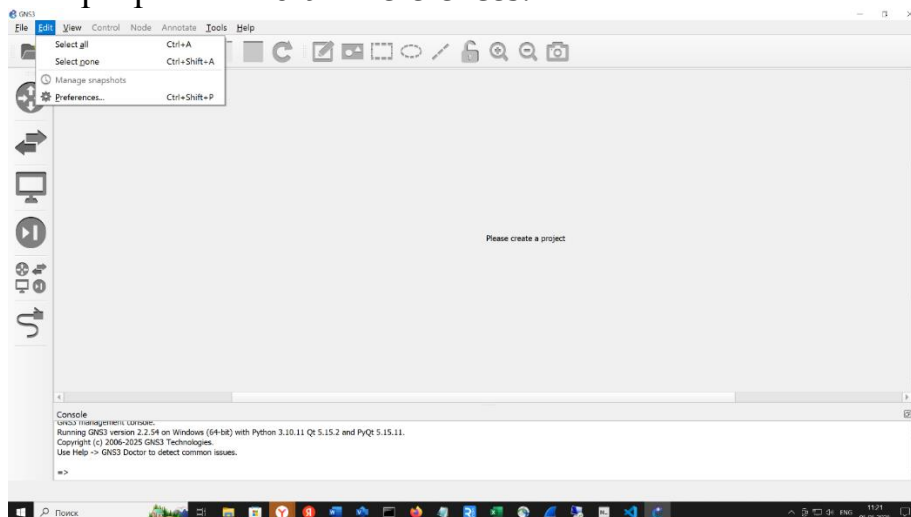


Рисунок 1-3. Экран выбора режима редактирования общих настроек в в программе GNS3.

Выбрать вкладки в главном меню Edit-Preferences далее выбрать вкладку Qemu VMS:

Лабораторные работы с виртуальным сервисным маршрутизатором vESR
В графическом симуляторе GNS3

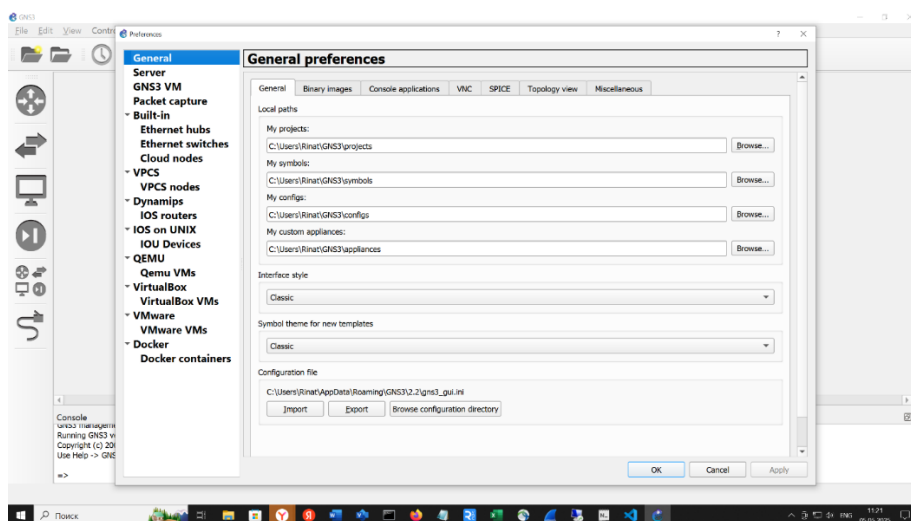


Рисунок 1-4. Настройка режима эмуляции с помощью виртуализации QEMU.

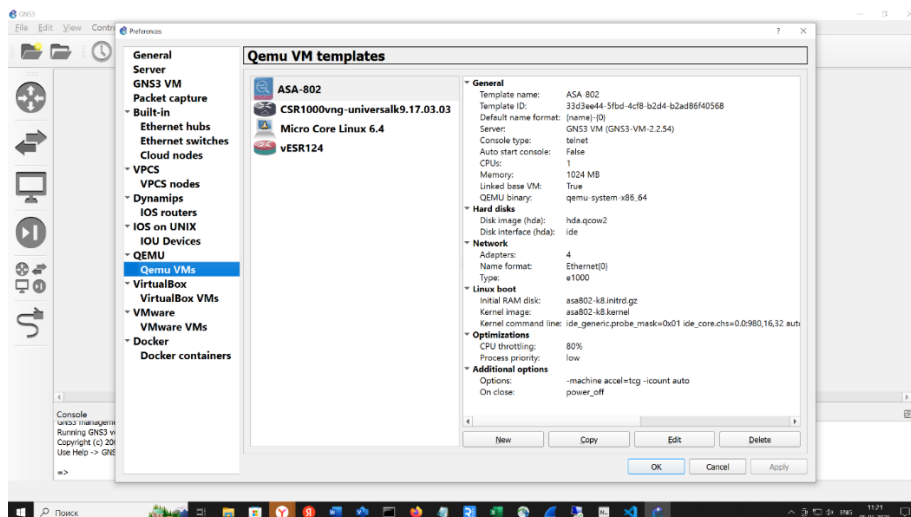


Рисунок 1-5. Экран настройки эмуляции нового сетевого устройства.

На этом экране нажать кнопку New для запуска следующих экранов установки образа. В этом процессе предстоит выбрать режим работы симулятора, название образа, количество сетевых адаптеров, памяти,

процессоров и источник на СД-РОМ:

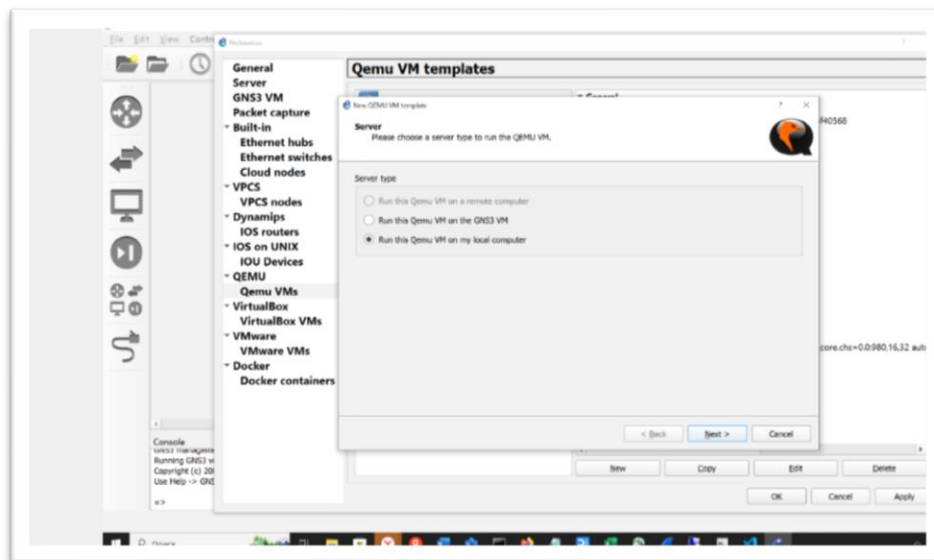


Рисунок 1-6. Экран выбора расположения эмулятора на хост машине.

Для работы рекомендуется запуск в специальной виртуальной машине, поставляемой вместе с симулятором. Кроме того, рекомендуется использовать для запуска этой виртуальной машины гипервизор VmWare Workstation 17.5. Установочный образ гипервизора довольно легко найти в сети и поставить в соответствии с рекомендациями нейросети. Рассмотрим простой сценарий установки VMware Workstation 17 Pro на компьютер с операционной системой Windows 10 или 11:

Скачать загрузочный файл программы с официального сайта.

Запустить установщик, выбрать «Run as administrator».

Дождаться, пока загрузятся необходимые файлы для установки новой версии VMware Pro.

Нажать кнопку «Next» в окне установки.

Принять лицензионное соглашение, после чего нажать кнопку «Next» в окне «Лицензионное соглашение конечного пользователя».

Установить расширенный драйвер клавиатуры, для этого нужно проверить поле подтверждения и нажать «Next». [2](#)

Включить автоматические обновления при запуске.

Лабораторные работы с виртуальным сервисным маршрутизатором vESR
В графическом симуляторе GNS3

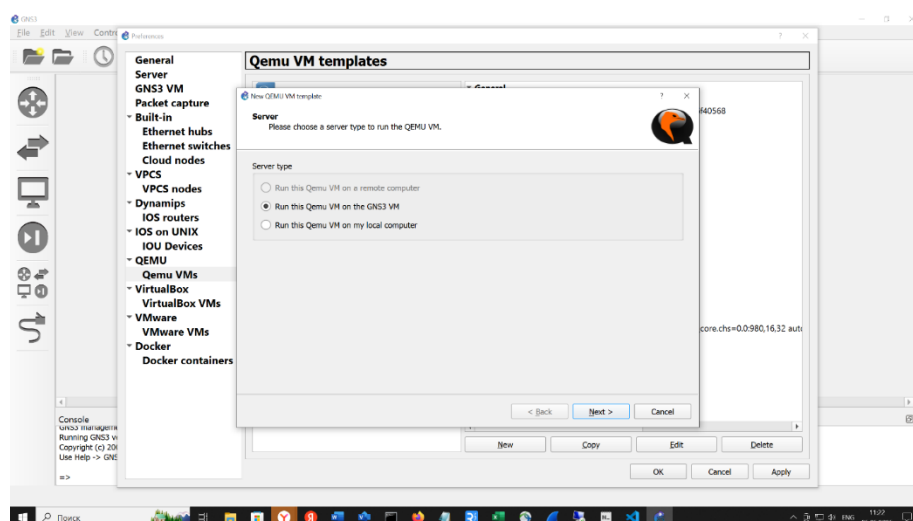


Рисунок 1-7. Экран выбора расположения эмулятора на виртуальной машине.

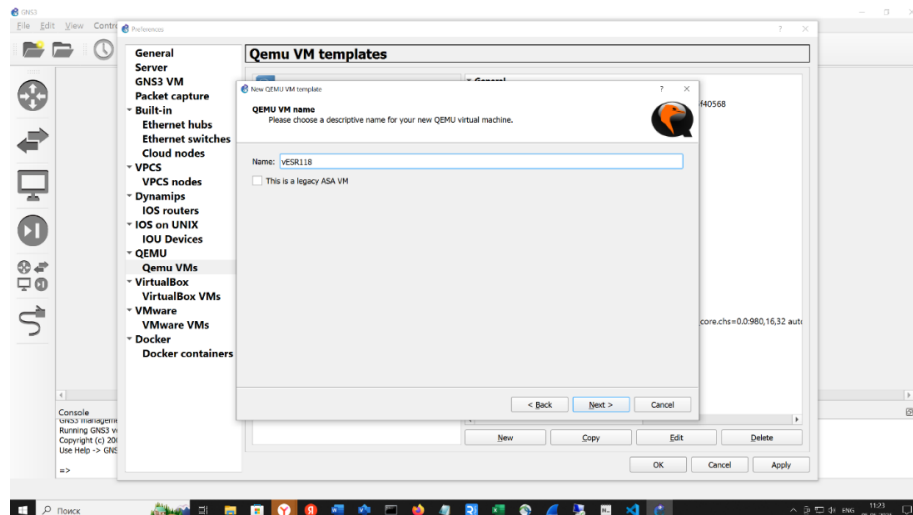


Рисунок 1-8. Экран ввода названия нового виртуального устройства.

Требуется дать название создаваемому образу. Для нормально й работы ему потребуется не менее 4 гигабайт оперативной памяти для работы виртуального маршрутизатора. Выбрать тип консоли VNC и идем далее -> Next :

Лабораторные работы с виртуальным сервисным маршрутизатором vESR
В графическом симуляторе GNS3

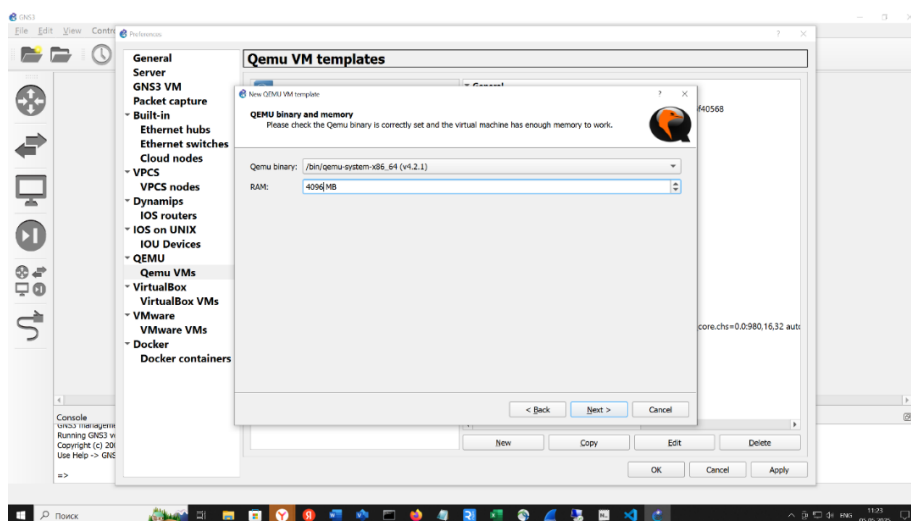


Рисунок 1-9 Экран ввода значений количества оперативной памяти.

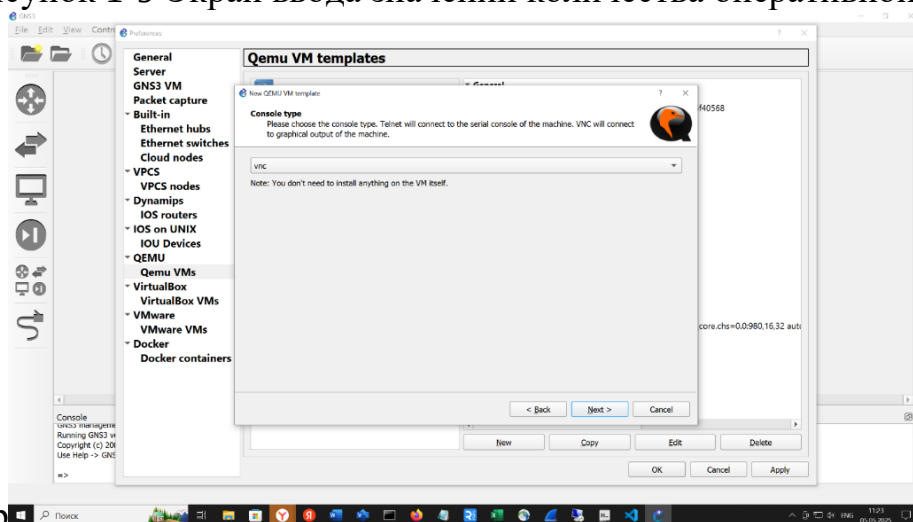


Рисунок 1-10. Экран выбора типа консоли.

Выбрать режим создания образа New Image -> дать имя vESR118 -
>Create -> Next

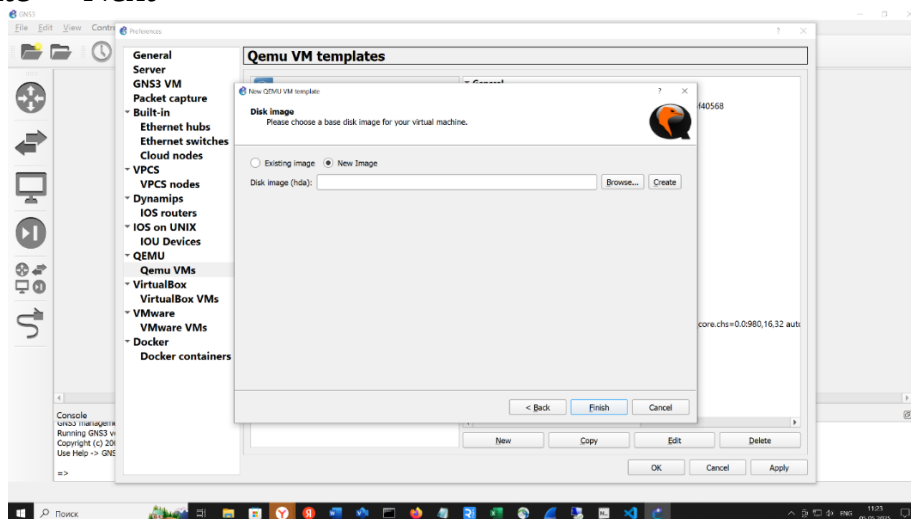


Рисунок 1-11. Экран выбора режима создания нового образа диска.

Лабораторные работы с виртуальным сервисным маршрутизатором vESR
В графическом симуляторе GNS3

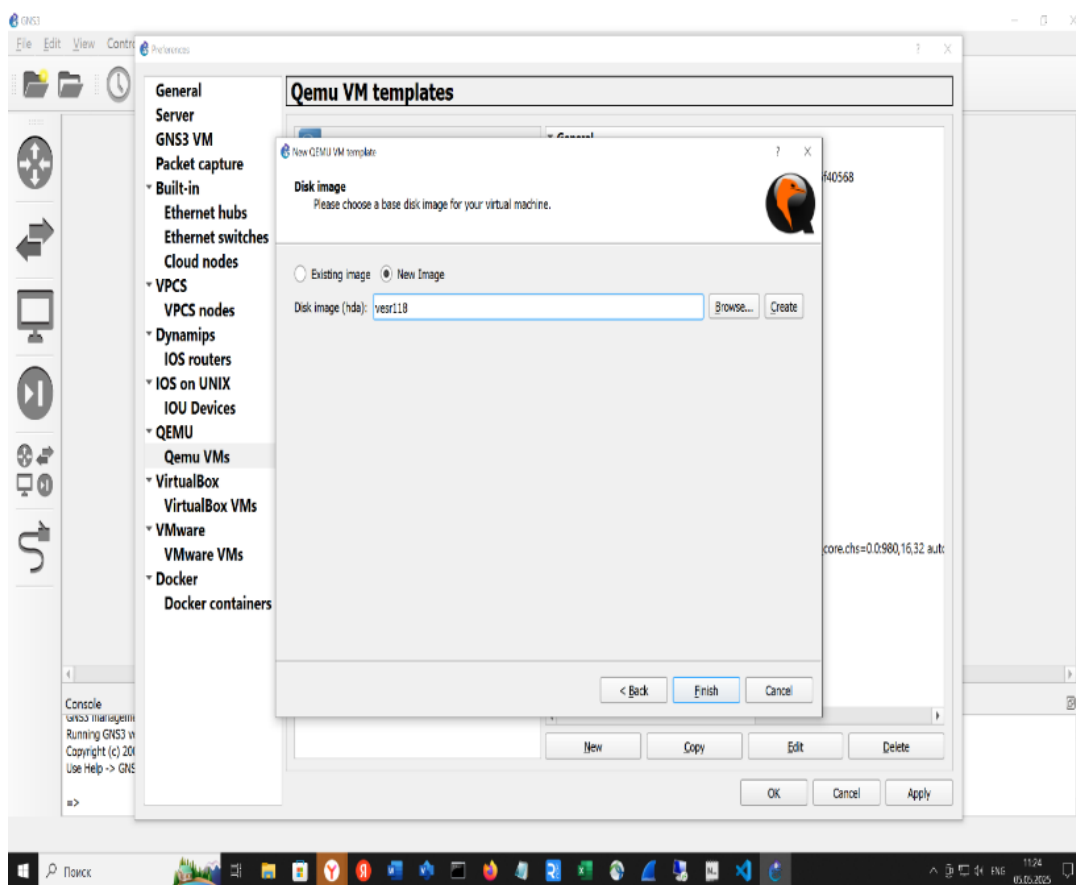


Рисунок 1-12. Экран ввода имени нового образа диска.
Выбрать формат образа -> Qcow2 -> Next

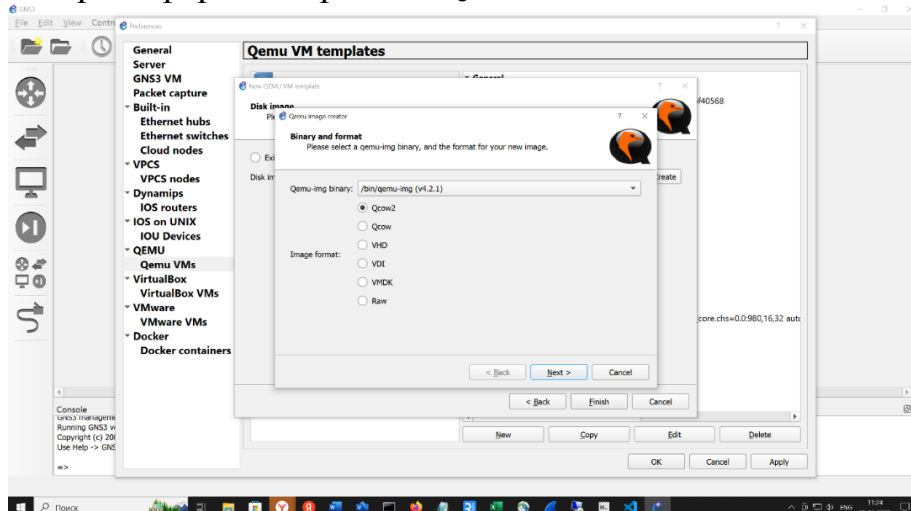


Рисунок 1-13. Экран выбора типа эмуляции.

Лабораторные работы с виртуальным сервисным маршрутизатором vESR
В графическом симуляторе GNS3

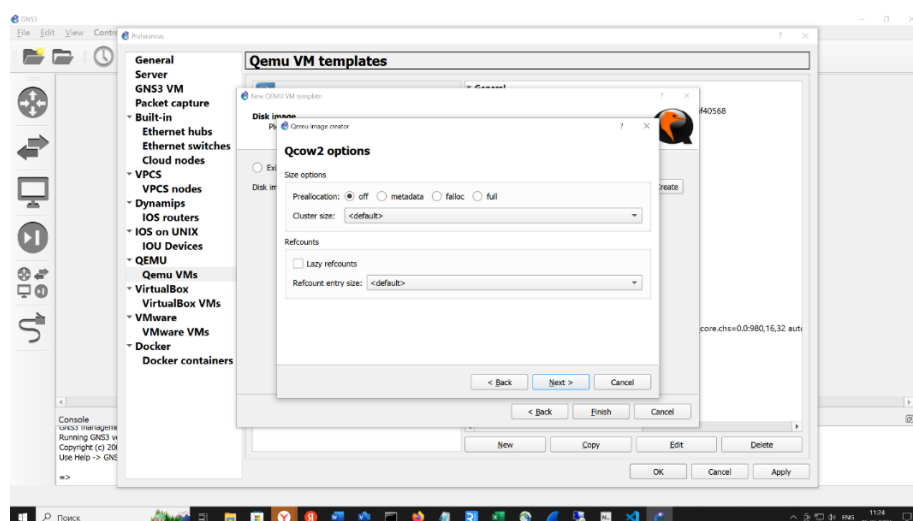


Рисунок 1-14. Экран выбора вариантов выбора режима.
Здесь ничего не меняем -> Next. Далее выделяем под размер образа 1 Гиг и нажимаем кнопку Finish.

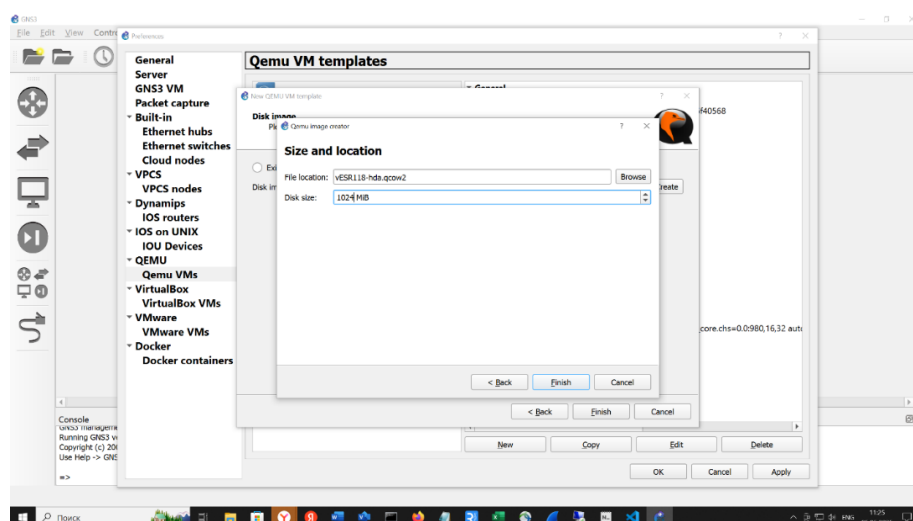


Рисунок 1-15. Экран ввода размера диска загрузочного образа.
Возвращаемся во вкладку Qemu VM Templates, выбираем образ vESR118 (или новее) и редактируем его настройки -> Edit (например 4 сетевые карты).

Там нужно отредактировать количество сетевых интерфейсов во вкладке Network и указать путь к исходному файлу с ISO образом виртуального маршрутизатора от производителя - CD-ROM.

Лабораторные работы с виртуальным сервисным маршрутизатором vESR
В графическом симуляторе GNS3

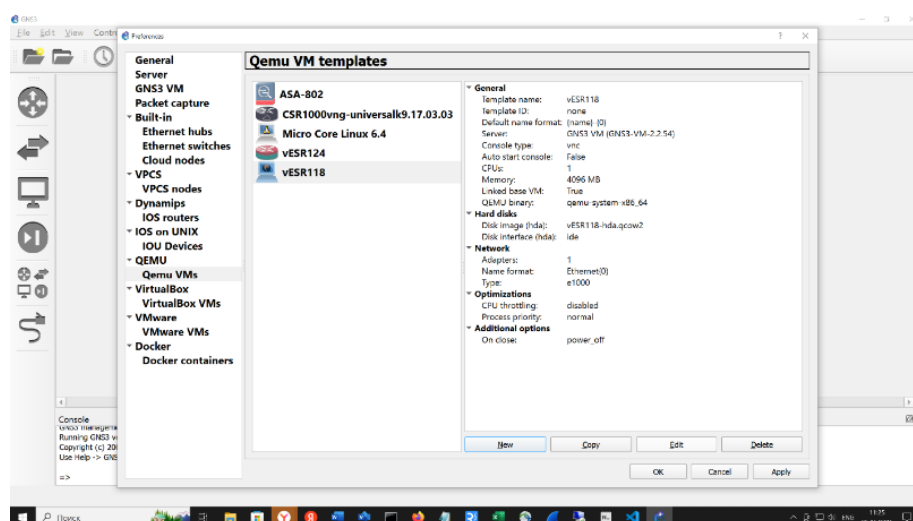


Рисунок 1-16. Экран настроек вновь созданного устройства.

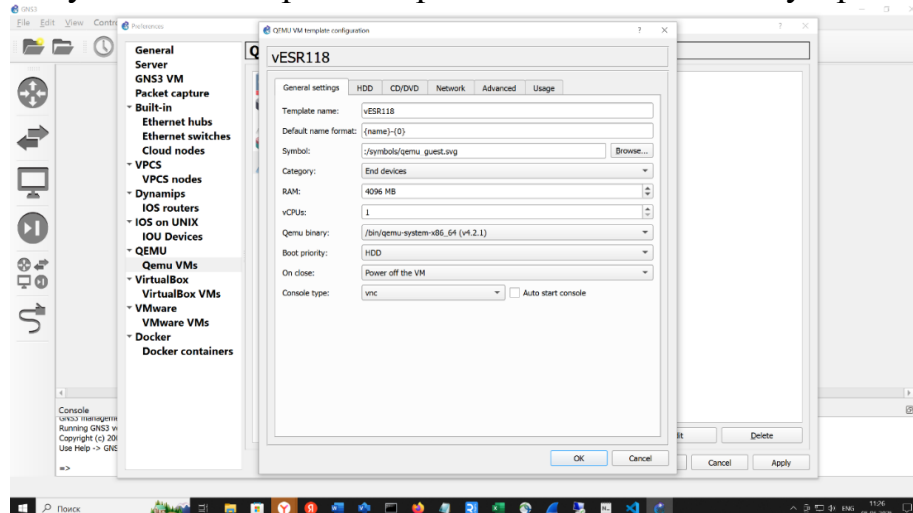


Рисунок 1-17. Экран настроек диска, сети и источника.

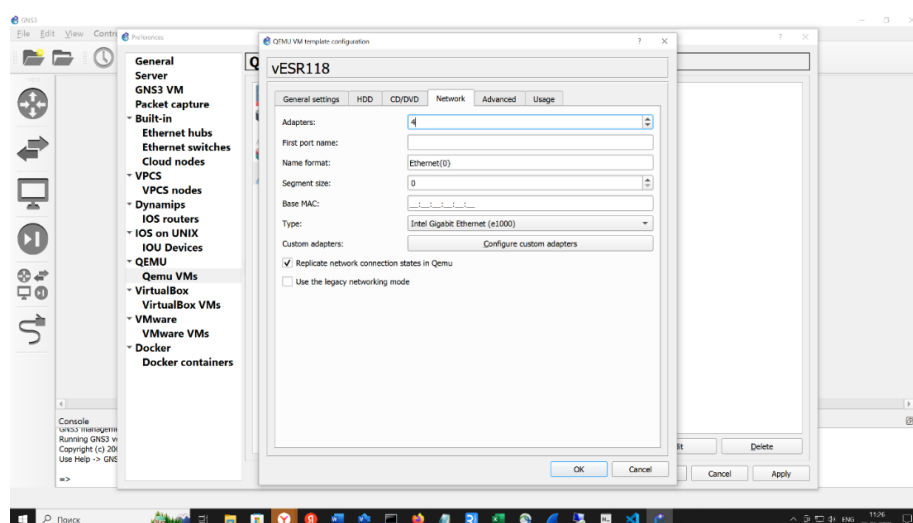


Рисунок 1-18. Экран добавления сетевых адаптеров.

Лабораторные работы с виртуальным сервисным маршрутизатором vESR
В графическом симуляторе GNS3

В поле Adapters поменять 1 на 4. В поле Image вкладки CD/DVD-ROM -> Browse -> Downloads -> cdrom.iso предварительно скачать из сети ISO или запросить с сайта производителя <https://eltex-co.ru/catalog/virtualnyi-servisnyi-marsrutizator-vesr/> (заполнив анкету) файл образа виртуального маршрутизатора.

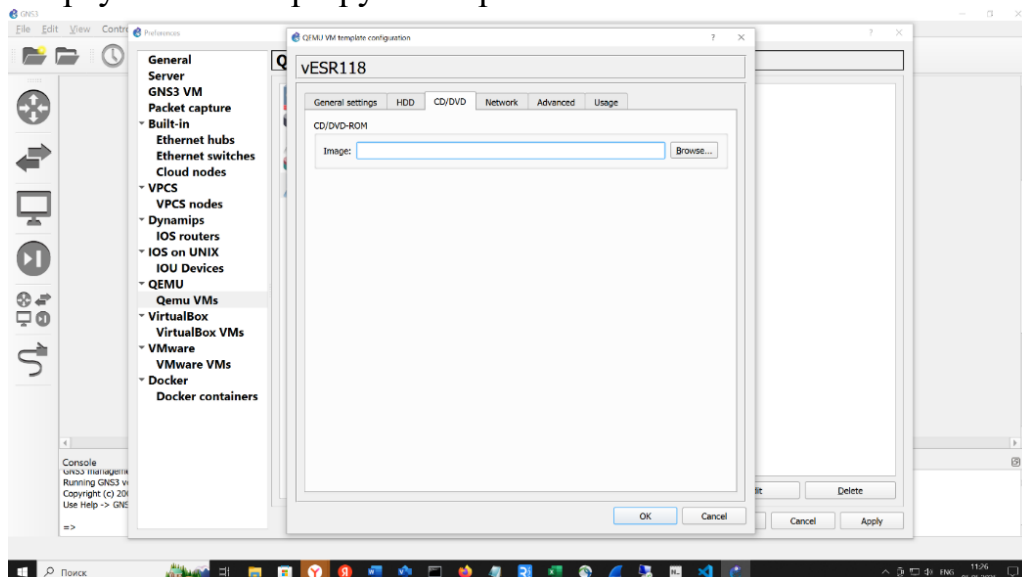


Рисунок 1-19. Экран выбора источника ISO образа.

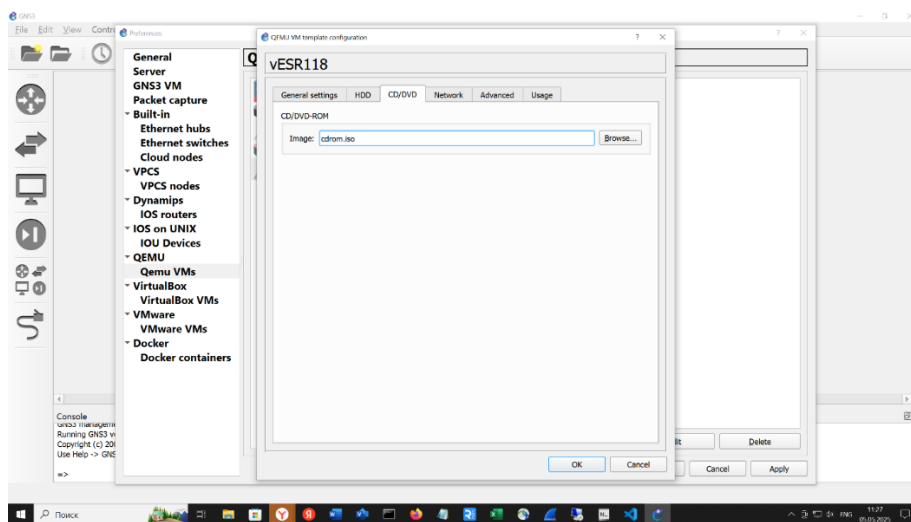


Рисунок 1-20. Экран установки источника образа.
Затем нажимаем на кнопку ОК.

Лабораторные работы с виртуальным сервисным маршрутизатором vESR
В графическом симуляторе GNS3

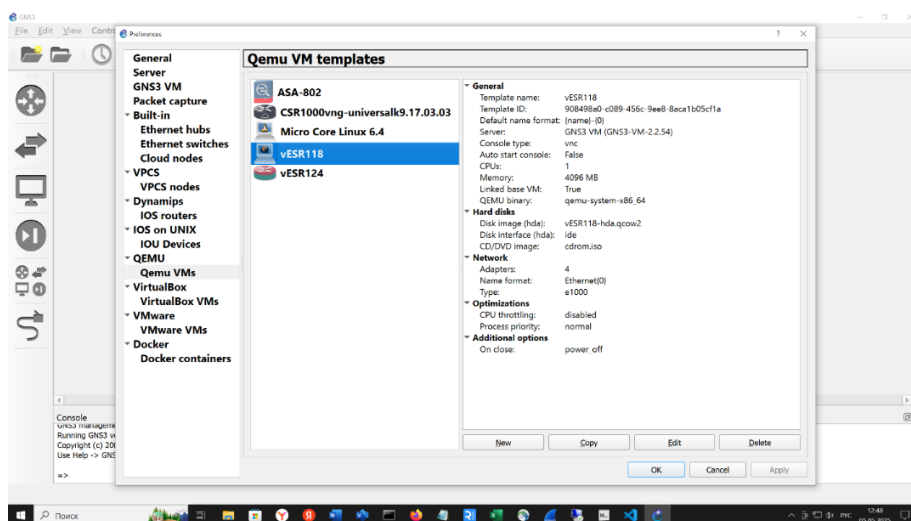


Рисунок 1-21. Экран подготовленного к работе устройства.

По умолчанию иконка маршрутизатора vESR124 будет в виде персонального компьютера. Это легко изменить. Наведите курсор на иконку с именем vESR24, нажмите правую клавишу мыши и выберите пункт меню **Configure Template**. Затем, в правом окне выберите строку **Symbol** и нажмите кнопку **Browse**, в появившемся подменю выберите строчку **Classic** и пролистайте до понравившейся вам иконке. Нажмите **OK**.

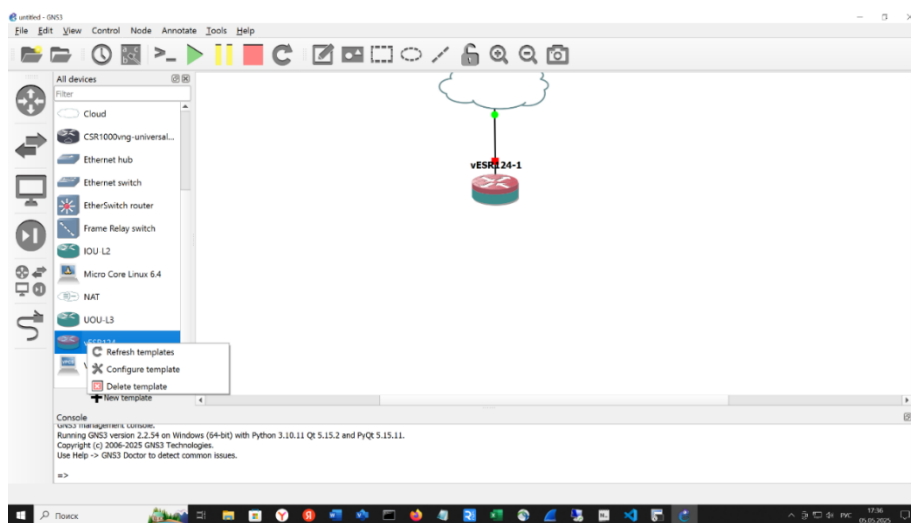


Рисунок 1-22. Экран настройки иконки устройства.

Лабораторные работы с виртуальным сервисным маршрутизатором vESR
В графическом симуляторе GNS3

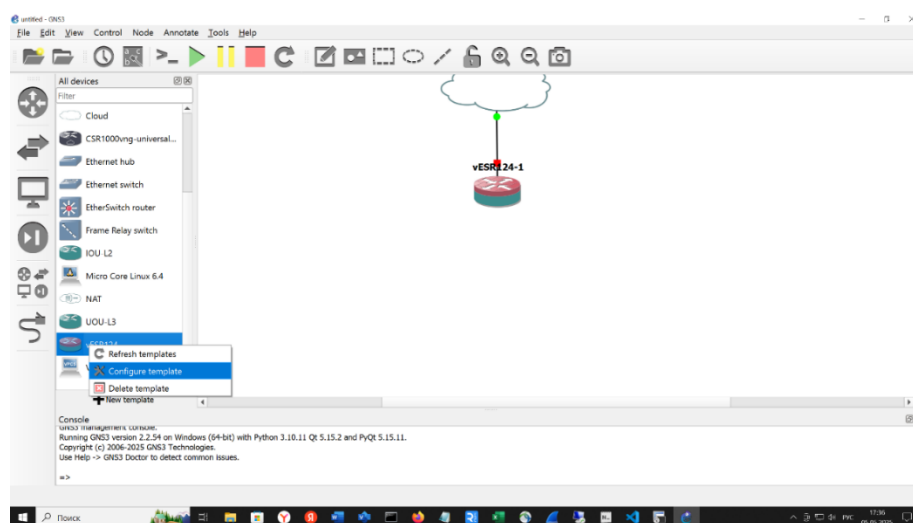


Рисунок 1-23. Экран настроек свойств устройства.

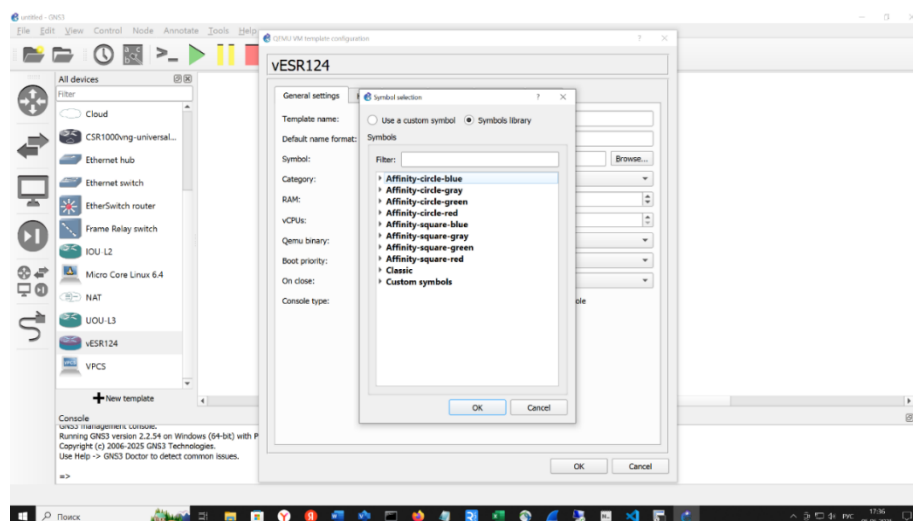


Рисунок 1-24. Экран с вариантами иконок.

Лабораторные работы с виртуальным сервисным маршрутизатором vESR В графическом симуляторе GNS3

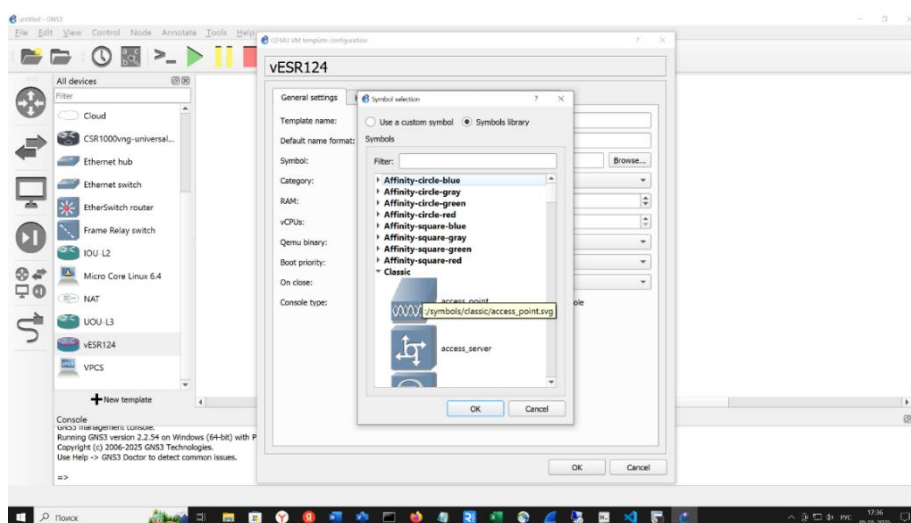


РИСУНОК 1-25. ЭКРАН С ИКОНКАМИ МАРШРУТИЗАТОРОВ И КОММУТАТОРОВ.

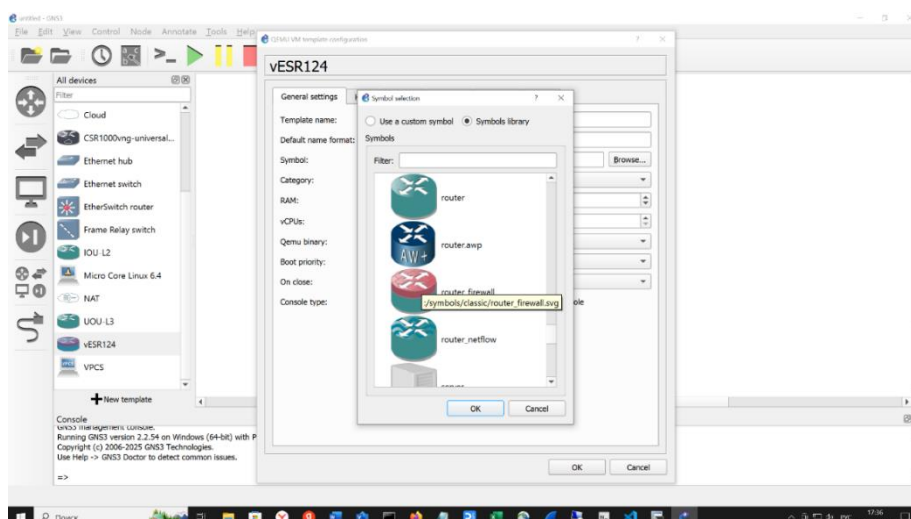


РИСУНОК 1-26. ЭКРАН ВЫБОРА НУЖНОЙ ИКОНКИ.

После этого образ можно использовать в лабораторных работах. Следует иметь в виду, что каждый новый объект vESR на схеме потребует отдельной инициации. Рассмотрим на примере простой схемы. Для создания этой схемы с помощью курсора мыши и зажатой левой клавиши мыши перетащите иконку с облаком, а затем иконку с маршрутизатором на правое поле. Точно так же методом перетаскивания объектов нужно соединить сетевые интерфейсы облака и маршрутизатора – сначала активировав иконку с кабелем (на иконке появится красный кружок с крестиком) а затем перенеся курсор в виде крестика на облако и нажав на левую кнопку мыши последовательно выбирая из списка порт соединяя устройства на схеме:

Лабораторные работы с виртуальным сервисным маршрутизатором vESR В графическом симуляторе GNS3

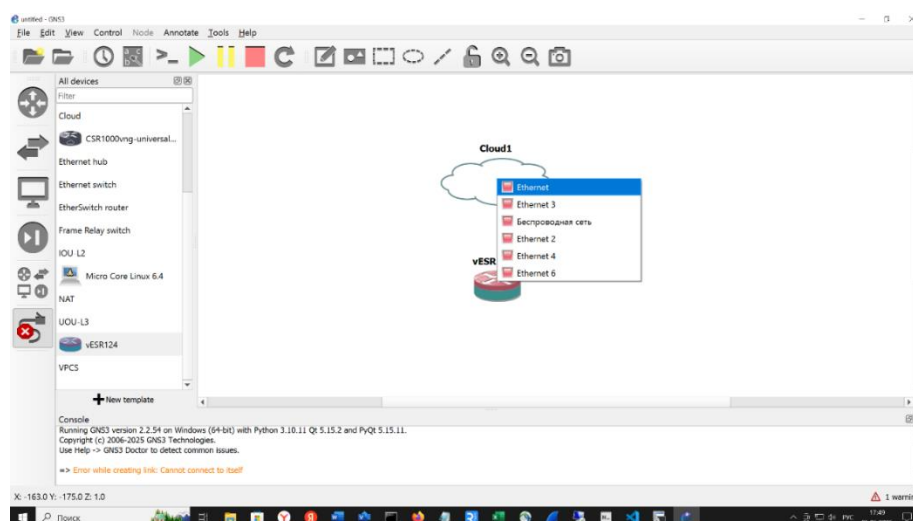


Рисунок 1-27. Экран создания схемы соединений.

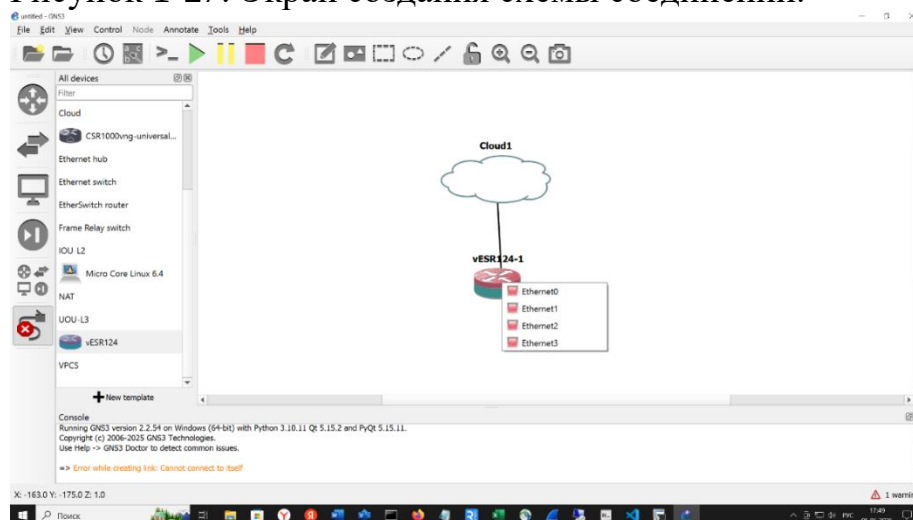


Рисунок 1-28. Экран выбора точек соединения.

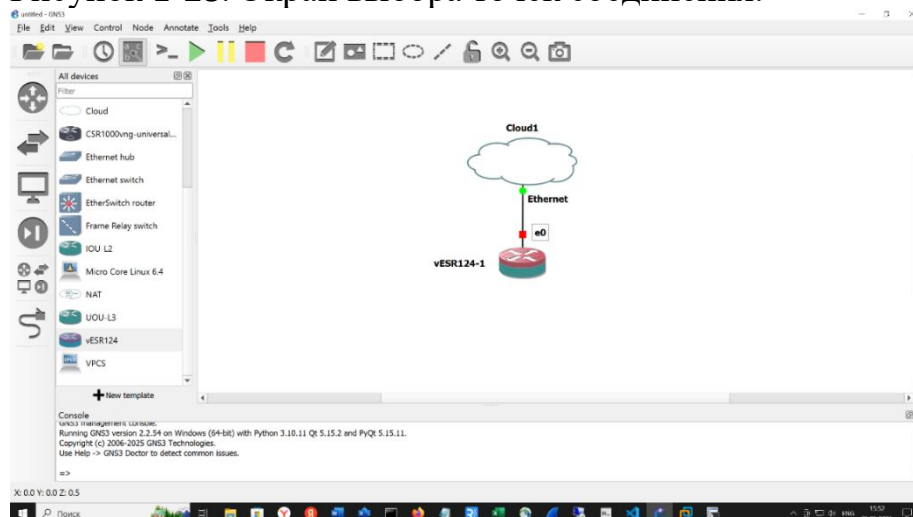


Рисунок 1-29. Экран созданной схемы с подключением.

Редактируем настройки этого устройства- установить автоматически запуск консоли VNS при старте. Это нужно для первоначальной установки системы, потом можно заменить на telnet для более комфортной работы с

Лабораторные работы с виртуальным сервисным маршрутизатором vESR
В графическом симуляторе GNS3

поддержкой выделения мышью и буфером обмена в программе Putty.
Autostart Console-> OK

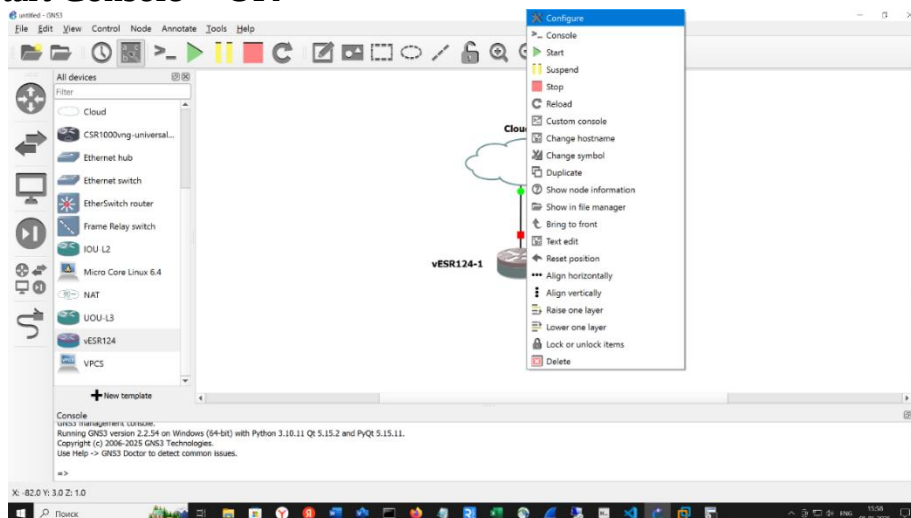


Рисунок 1-30. Экран вызова меню настроек устройства.

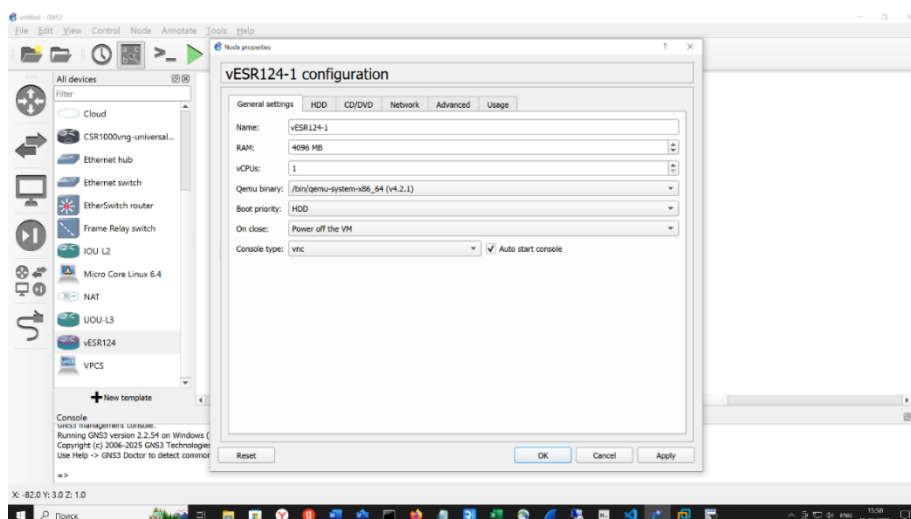


Рисунок 1-31.Экран с меню конфигурации.

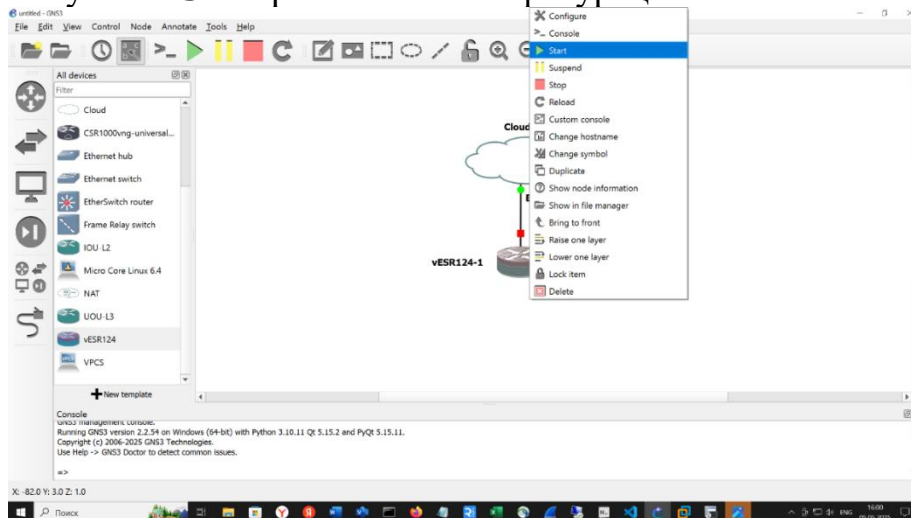


Рисунок 1-32. Экран запуска устройства.

Должно открыться окно терминала UltraVNC. Дождитесь окончания таймера или нажмите "Enter".

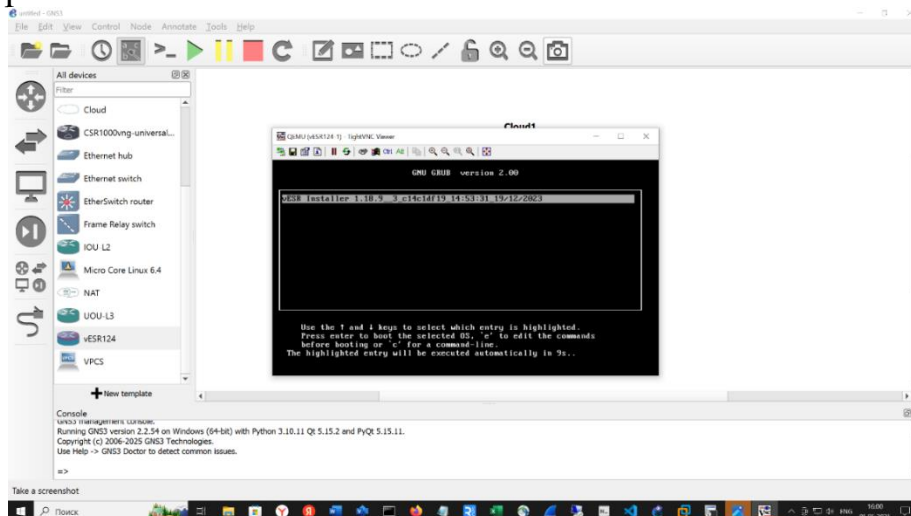


Рисунок 1-33. Экран запуска инициации маршрутизатора. Используя клавиши "↑, ↓", выберите пункт "vESR Installation". Используя клавиши "←, →", выберите пункт "OK" и нажмите клавишу "Enter".

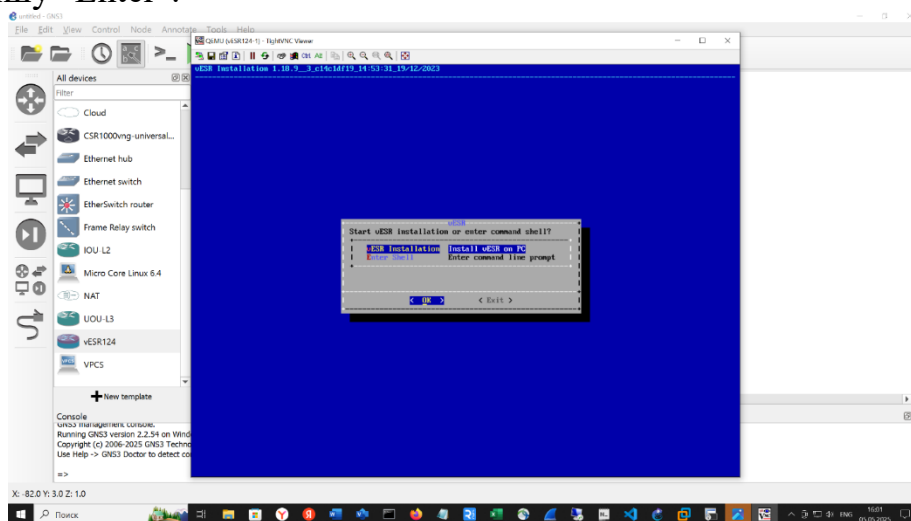


Рисунок 1-34. Экран выбора параметров размера диска под СИСТЕМУ.

Нажмите клавишу "Space", в левом поле появится символ "*". Используя клавиши "←, →", выберите пункт "OK" и нажмите клавишу "Enter".

Лабораторные работы с виртуальным сервисным маршрутизатором vESR В графическом симуляторе GNS3

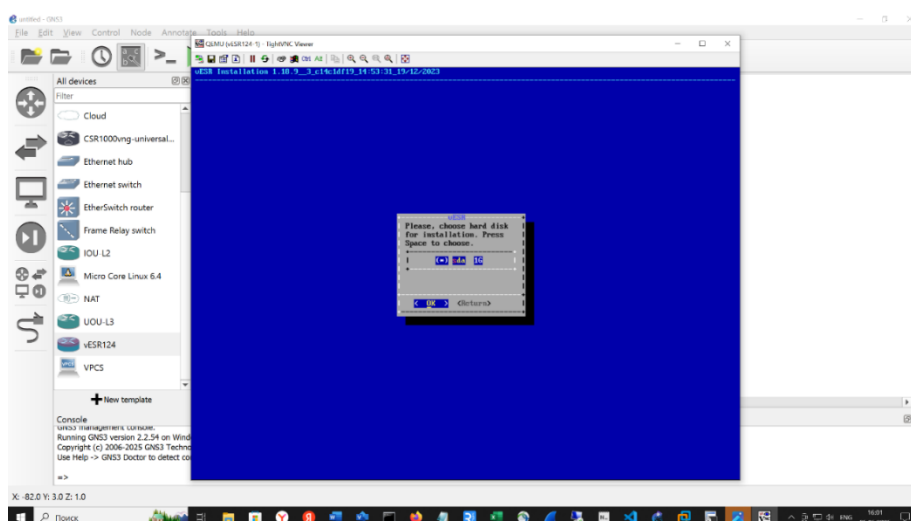


РИСУНОК 1-35. ЭКРАН ВЫБОРА РАЗМЕРА ДИСКА.

Используя клавиши "←, →", выберите пункт "OK" и нажмите клавишу "Enter".

После установки вы увидите надпись "Installation complete. Please, reboot".

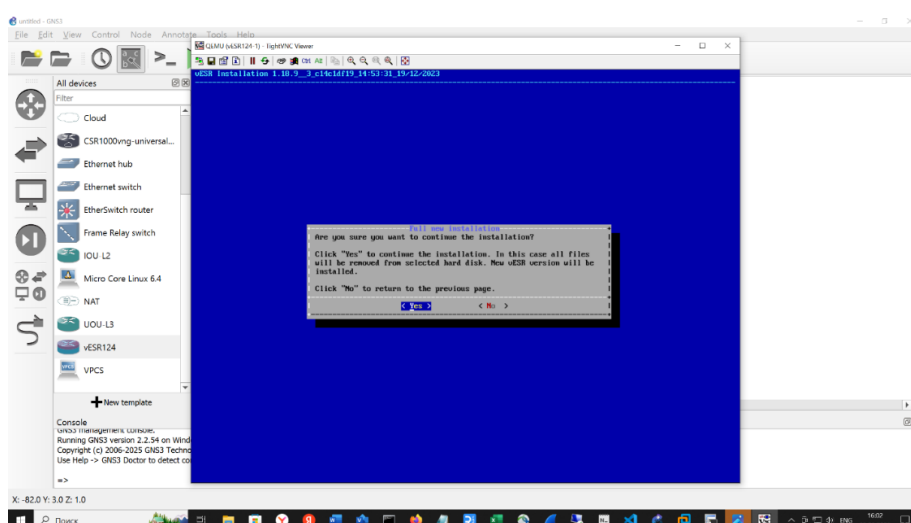


РИСУНОК 1-36. ЭКРАН ЗАВЕРШЕНИЯ ПЕРВОНАЧАЛЬНЫХ НАСТРОЕК ПАРАМЕТРОВ.

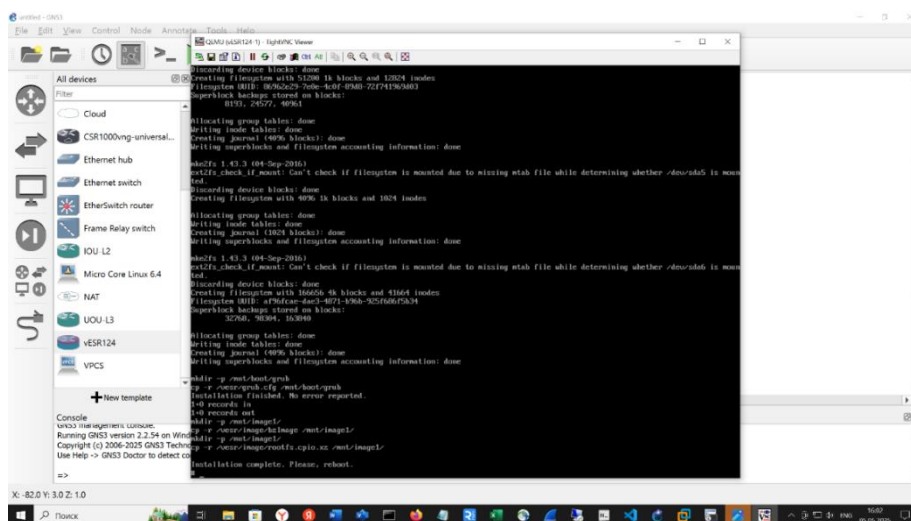


РИСУНОК 1-37. ЭКРАН ЖУРНАЛА СООБЩЕНИЙ ПРИ ИНИЦИАЛИЗАЦИИ ОБРАЗА.

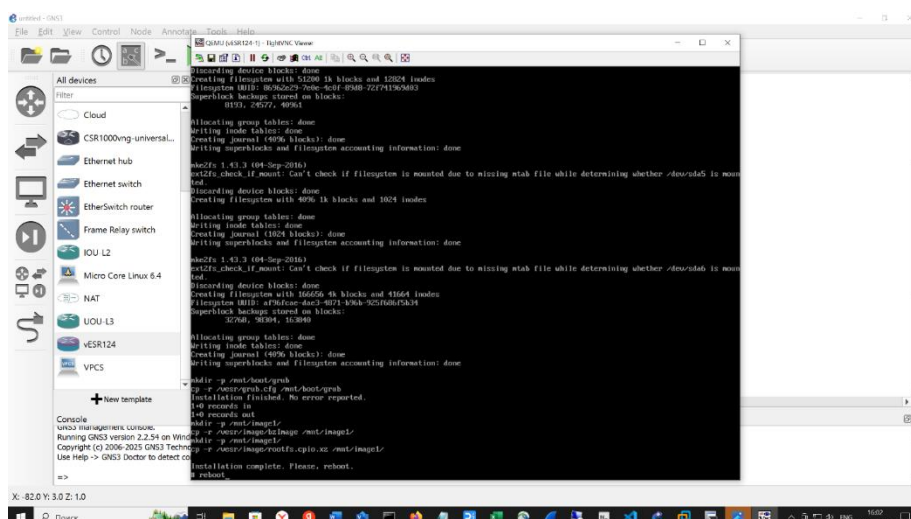


РИСУНОК 1-38. ЭКРАН ЗАВЕРШЕНИЯ ИНИЦИАЦИИ И ПРЕДЛОЖЕНИЕ ПЕРЕЗАГРУЗКИ.

Лабораторные работы с виртуальным сервисным маршрутизатором vESR В графическом симуляторе GNS3

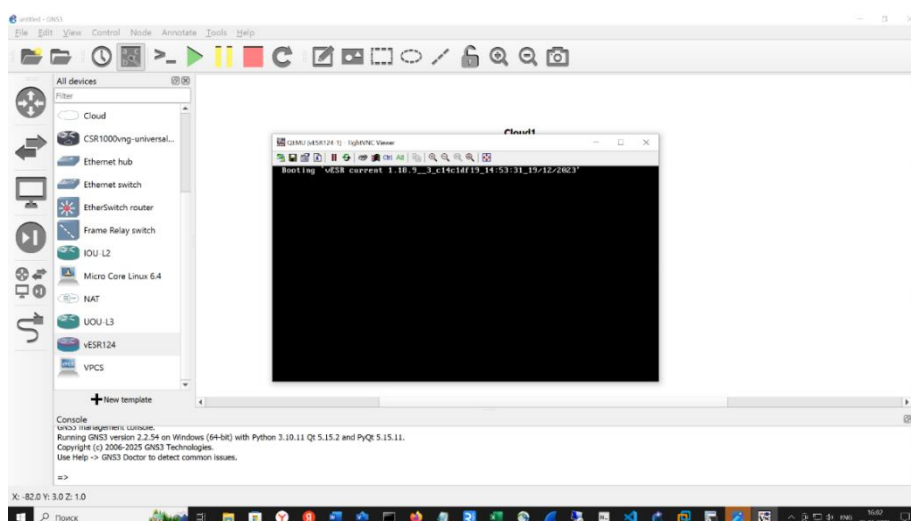


РИСУНОК 1-39. ЭКРАН ЗАГРУЗКИ МАРШРУТИЗАТОРА.

После перезагрузки командой `reboot` нужно выйти из консоли (например, нажав крестик в правом верхнем углу экрана консоли VNC) и маршрутизатор нужно остановить (правая кнопка мыши -> Stop или нажать на красный квадрат в верхнем меню программы GNS3, затем зайти во вкладку Configure (навести курсор мыши на иконку маршрутизатора vESR124-1, нажать правую клавишу мыши – выбрать Configure) и заменить программу консоли на telnet, нажать на кнопку ОК для выхода и заново запустить маршрутизатор, как показано на рисунках ниже :

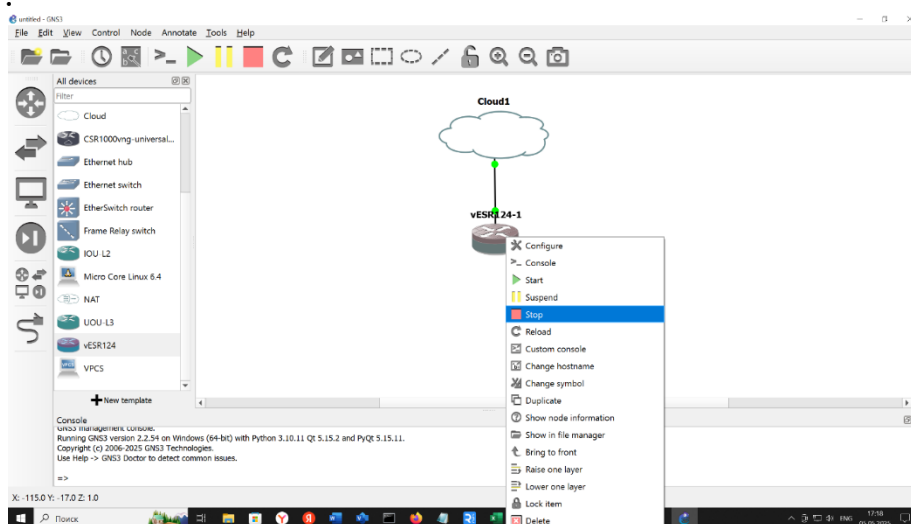


РИСУНОК 1-40. ЭКРАН ВЫБОРА ТИПА КОНСОЛИ ПРИ ЗАГРУЗКЕ МАРШРУТИЗАТОРА.

Лабораторные работы с виртуальным сервисным маршрутизатором vESR В графическом симуляторе GNS3

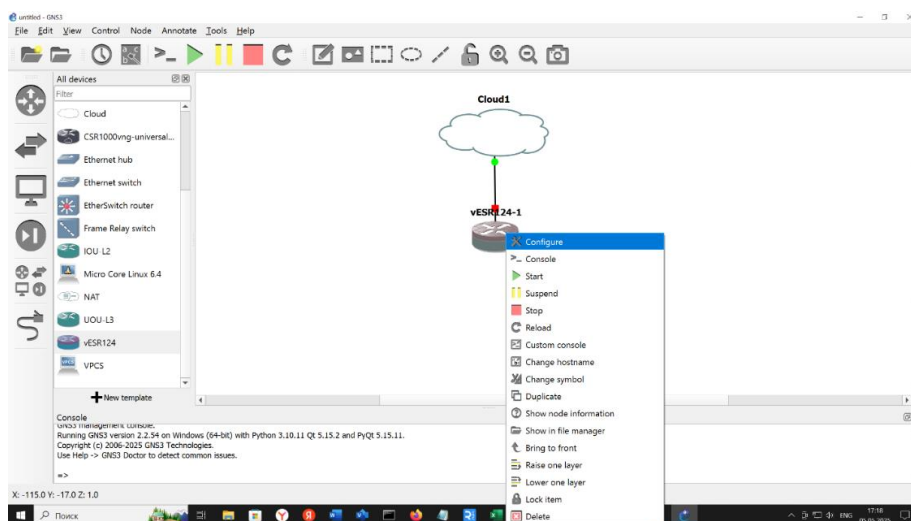


Рисунок 1-41. Э/КРАН НАСТРОЕК КОНФИГУРАЦИИ.

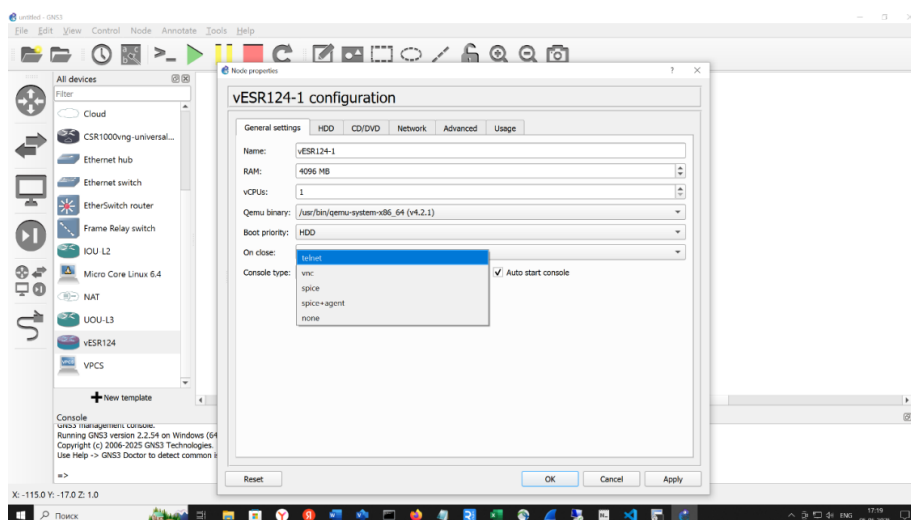


Рисунок 1-42. ЭКРАН ВЫБОРА КОНСОЛИ.

Далее стартовать маршрутизатор нажав на зеленый треугольник в главном меню программы GNS3 или установив курсор мыши на иконку маршрутизатора vESR124-1 и нажав правую клавишу мыши для вызова контекстного меню и выбрав пункт Start.

При старте автоматически откроется окно терминала Putty. И спустя некоторое время (зависит от быстродействия и загрузки процессора вашего компьютера, появится приглашение на ввод логина и пароля. Начальные установки Логин – admin, Пароль – password

Лабораторные работы с виртуальным сервисным маршрутизатором vESR
В графическом симуляторе GNS3

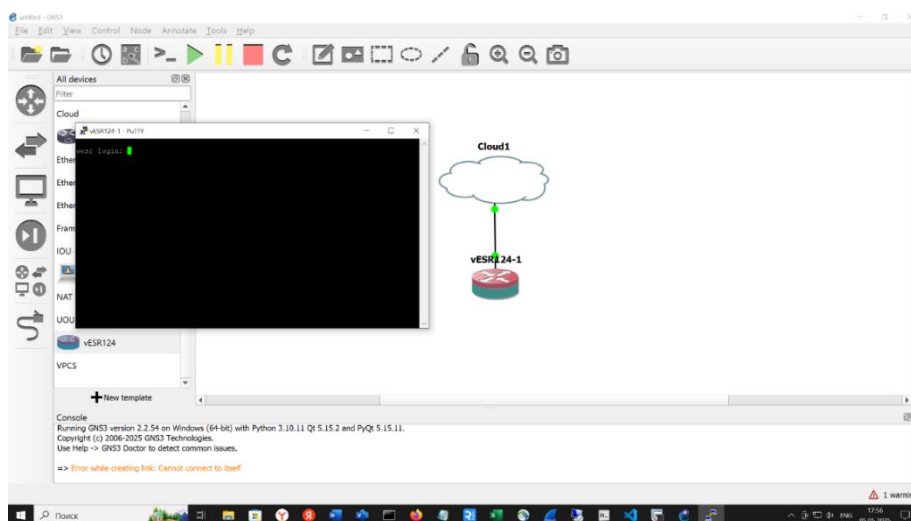


РИСУНОК 1-43. ЭКРАН ЗАГРУЗКИ МАРШРУТИЗАТОРА (ДОЛГО).

В результате будет получен такой вывод:

vesr login: **admin**

Password:password

You are required to change your password immediately!!!

* Welcome to vESR *

vesr(change-expired-password)#

vesr(change-expired-password)# **password eve**

vesr(change-expired-password)# commit

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

vesr(change-expired-password)# confirm

Configuration has been confirmed. Commit timer canceled.

vesr# config

vesr(config)# hostname vesr124-1

vesr(config)# exit

Warning: you have uncommitted configuration changes.

vesr# commit

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

vesr124-1# confirm

Configuration has been confirmed. Commit timer canceled.

vesr124-1# save

Configuration has been successfully saved

vesr124-1#

```
vesr124-1#
vesr124-1# sh running-config
hostname vesr124-1
syslog max-files 3
syslog file-size 512
syslog file tmpsys:syslog/default
severity info
exit
username admin
password encrypted
$6$Kx1jB3DT6zH05CQ7$WqbKGSvl/35jvx.NKDc6R5NpD5uy2623zfbWAO
TPhNOQgnR.zXxQzlgYwESdbOxOWSyhPPNojy0Q0.pMvR6Ld/
exit
domain lookup enable
security passwords default-expired
ip ssh server
ntp enable
ntp broadcast-client enable
licence-manager
host address elm.eltex-co.ru
exit
vesr124-1#
```

Теперь маршрутизатор готов к работе и дальнейшей настройке.
Для дальнейшей работы сохраните проект под с названием,
например, vesr-book-base: Клавишами <- -> или мышью выделите Пункт
меню “File”, затем в выпадающем меню выберите пункт “Save project as
...” – и у вас откроется окно с выбором места где будет сохранен проект и
выбор его имени:

Лабораторные работы с виртуальным сервисным маршрутизатором vESR
В графическом симуляторе GNS3

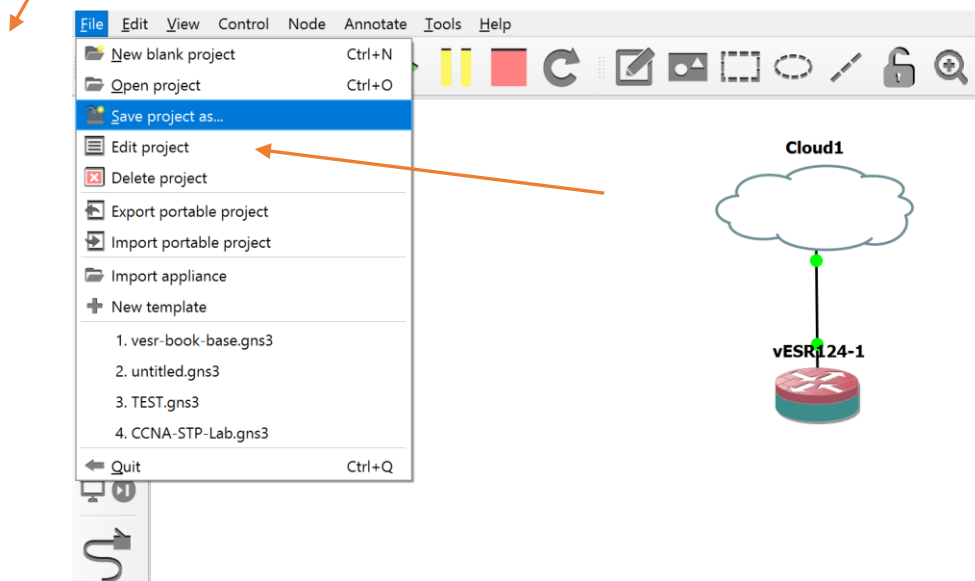


РИСУНОК 1-44. ЭКРАН НАСТРОЙКИ ПРОЕКТА.

Например так :

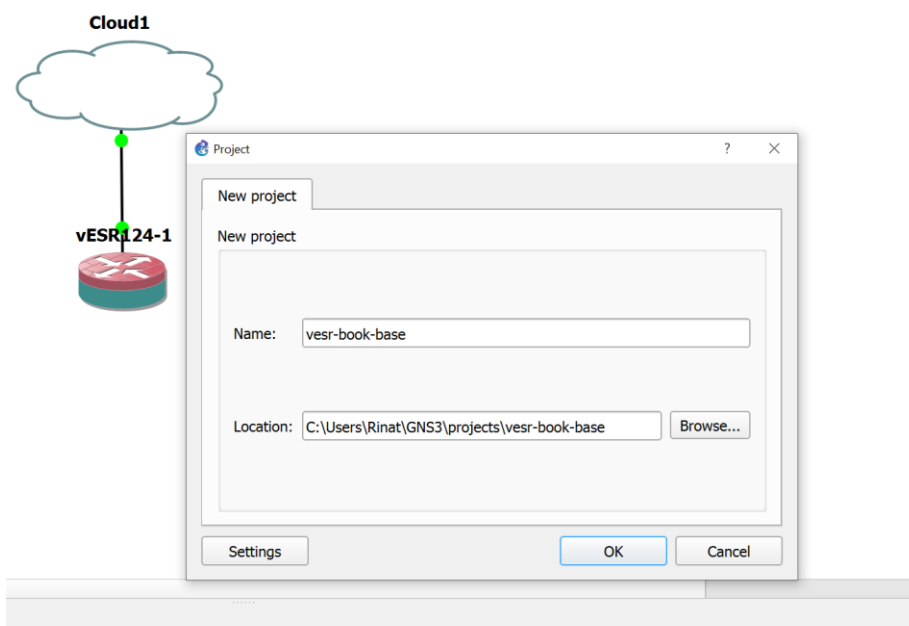


РИСУНОК 1-45. ЭКРАН ВВОДА ИМЕНИ. У ВАС МОЖЕТ БЫТЬ СВОЕ ИМЯ.

И нажмите клавишу ОК для сохранения.

ВЫВОДЫ ПО ГЛАВЕ

- Описано назначение и источник установки графического сетевого симулятора GNS3
- Приведен список требуемого дополнительного программного обеспечения
- Краткое описание установки программы VMware Workstation Pro 17.5
- По шагам расписана процедура настройки виртуальной машины GNS3
- Описана процедура установки нового устройства vesi в список встроенных в GNS3

В следующей главе вы узнаете почему выбор симулятора GNS3 предпочтительнее популярной программы EVE-NG.

Глава 2. Почему GNS3, а не EVE-NG?

При всей мощности **EVE-NG**, его использование требует:

- **Больших ресурсов:** Жёсткие требования к CPU/RAM, особенно для сложных топологий.
- **Сложности установки:** Необходимость настройки серверной версии для полноценной работы.
- **Ограниченная поддержка Windows:** EVE-NG лучше работает под Linux, что не всегда удобно для начинающих.

GNS3, особенно с **локальным гипервизором (VMware Workstation)**, выигрывает у EVE-NG по таким критериям:

- Легковесность на простых схемах (например, для лабораторных работ с 1-2 маршрутизаторами).
- Простота интерфейса и интеграции с Windows-инструментами (PuTTY, UltraVNC).

Гибкость: поддержка как QEMU (для vESR), так и Docker (для микросервисов), кстати в магазине приложений GNS3 есть бесплатные и легко доверяемые в набор предустановленных устройств в виде docker образов.

Совет читателям: Если вы планируете масштабные проекты (50+ устройств), со временем изучите EVE-NG Pro. Но для старта и большинства практических задач GNS3 + vESR — идеальный тандем.

ВЫВОДЫ ПО ГЛАВЕ

- GNS3 vs EVE-NG
- В чем преимущество GNS3

В следующей главе вы узнаете про базовые настройки виртуального сервисного маршрутизатора vESR.

Глава 3. Базовая настройка виртуального маршрутизаторе vESR.

Цель этой работы:

Изучить базовую настройку виртуального сервисного маршрутизатора vESR.

В программе GNS3 после запуска и спустя некоторое время, предназначенное для запуска виртуальной машины (признаком успешного старта будет появление через две-три минуты (зависит от мощности вашего оборудования) в верхнем левом углу панели программы зеленого информационного табло) открываем папку с проектом vesr-book-base следуя последовательности нажатий клавиш на пунктах меню “File”- “Open Project”

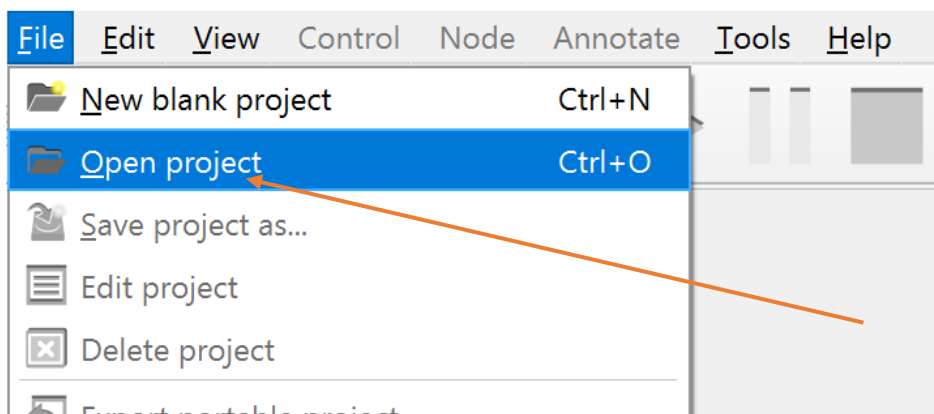


РИСУНОК 3-1. ЭКРАН РАБОТЫ С ПРОЕКТАМИ.

Откроется папка на диске, настроенная по умолчанию на который вы поместили программу GNS3 при установке, например такая:

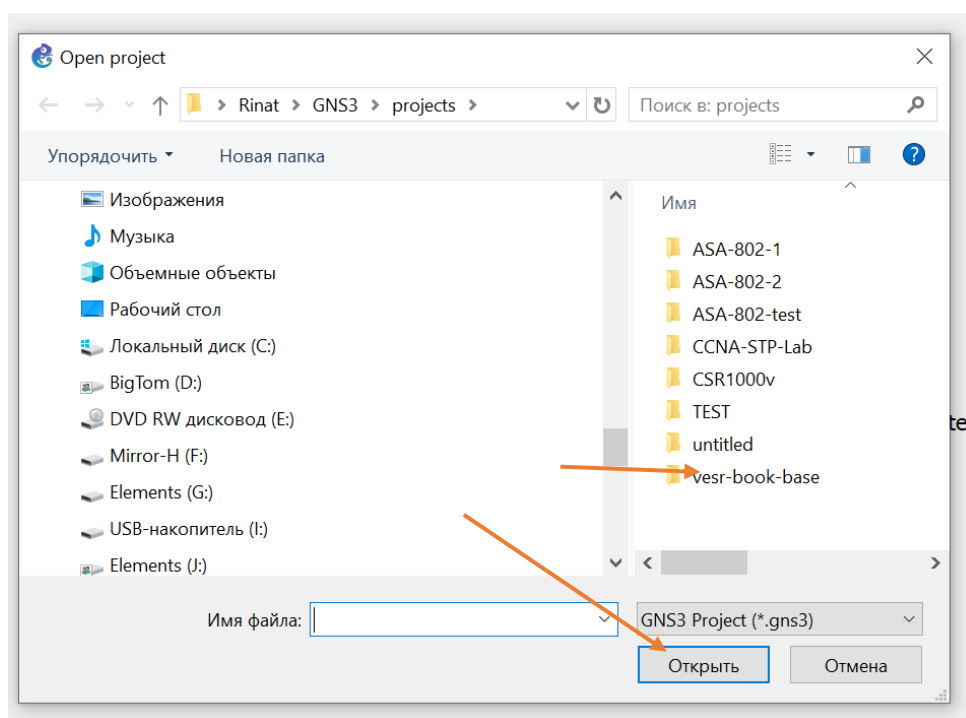


РИСУНОК 3-2. ЭКРАН ВЫБОРА ПРОЕКТА.

Для открытия проекта выбираете мышью vesr-book-base (у вас может быть другое имя), нажимаете на «Открыть».

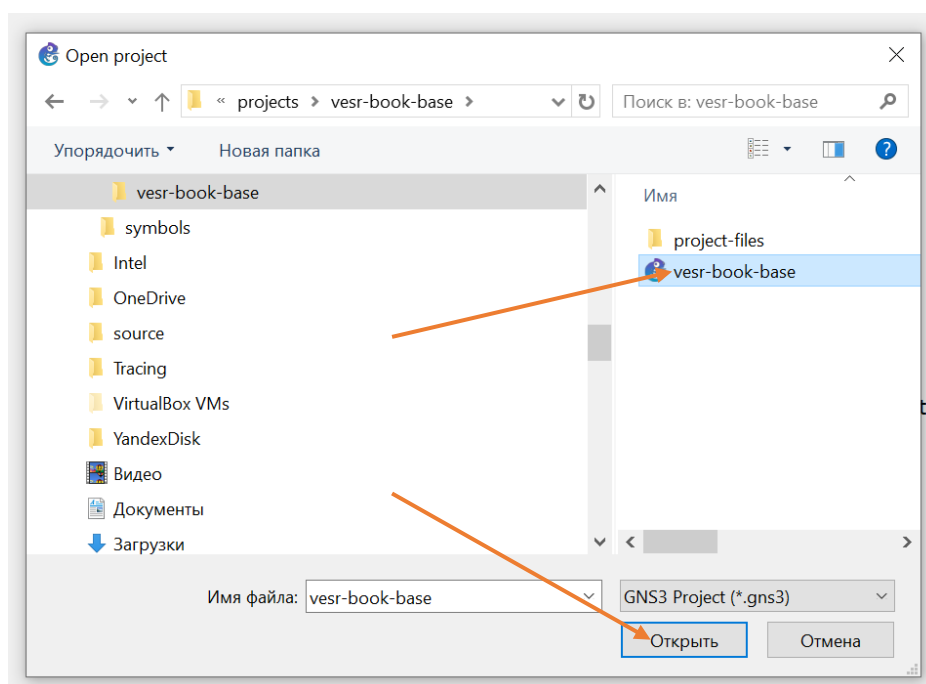


РИСУНОК 3-3. ЭКРАН ВЫБОРА ПРОЕКТА.

Такой же эффект можно получить и просто нажав курсором мыши на иконку открытой папки на навигационной панели GNS3.

Наводим курсор мыши на иконку маршрутизатора, нажимаем правую кнопку мыши и затем еще раз нажимаем на зеленый треугольник для старта нашего устройства.

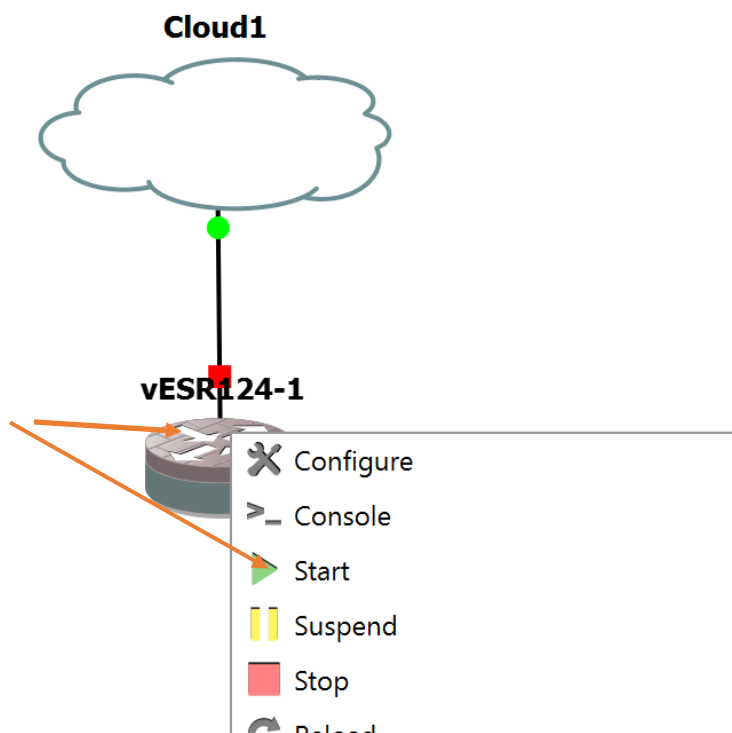


РИСУНОК 3.4. ЭКРАН УПРАВЛЕНИЯ ЗАПУСКОМ УСТРОЙСТВА.

Запускается консоль Putty (вы же при начальной конфигурации маршрутизатора в первой главе не забыли поставить галочку , указывающую на автоматический старт консоли?).

Ждем некоторое время – на моем домашнем ПК с 32 Гб и процессором 12th Gen Intel(R) Core(TM) i5-12500 3.00 GHz оно равно более минуты.

Если через более продолжительное время вы не получили приглашение в консоли на ввод логины, то вам следует вернуться к первоначальной установке маршрутизатора (измените тип консоли на VNC, чтобы увидеть процесс первоначальной загрузки, возможно там будут диагностические сообщения с подсказками).

И так вы в консоли- что дальше? Вводите логин-admin и пароль- eve (его мы установили на этапе первоначальной настройки).

```
vesr124-2-1 login: admin
Password:
```

```
*****
*           Welcome to vESR           *
*****
```

```
vesr124-2-1#
```

Процедура базовой настройки маршрутизатора состоит из следующих этапов:

- Создание новых пользователей
- Назначение имени устройства
- Установка параметров подключения к публичной сети (WAN) и локальной сети (LAN)
- Настройка проверки связности через ICMP

• Создание новых пользователей

Для создания нового пользователя системы или настройки любого из параметров: имени пользователя, пароля, уровня привилегий, – используются команды:

```
username <name>
password <password>
privilege <privilege>
exit
```

где:

<name> - имя нового пользователя;

<password> - пароль для нового пользователя

<privilege> - № от 1 до 15

Уровни привилегий 1-9 разрешают доступ к устройству и просмотр его оперативного состояния, но запрещают настройку. Уровни привилегий 10-14 разрешают как доступ, так и настройку большей части функций устройства. Уровень привилегий 15 разрешает как доступ, так и настройку всех функций устройства.

Пример:

создание пользователя "Rinat" с паролем "P@ssw0rd" и максимальными привилегиями (15)

```
vesrl24-1#
vesrl24-1# config
vesrl24-1(config)# username rinat
vesrl24-1(config-user)# password P@ssw0rd
vesrl24-1(config-user)# privilege 15
vesrl24-1(config-user)# exit
vesrl24-1(config)# do commit
Configuration has been successfully applied and saved to flash. Commit timer started, changes will be reverted in 600 seconds.
vesrl24-1(config)# do confirm
Configuration has been confirmed. Commit timer canceled.
vesrl24-1(config)# exit
vesrl24-1#
```

РИСУНОК 3-4. ЭКРАН СОЗДАНИЯ НОВОГО ПОЛЬЗОВАТЕЛЯ В СИСТЕМЕ.

Для применения настроек:

```
do commit
```

```
do confirm
```

Проверка входа из под пользователя "rinat":

```
vesr124-1# exit
vesr124-1 login: rinat
Password:

*****
*                               *
*      Welcome to vESR          *
*                               *
*****
vesr124-1#
```

РИСУНОК 3-5. ЭКРАН ВХОДА В СИСТЕМУ ПОД НОВЫМ ПОЛЬЗОВАТЕЛЕМ.

- **Назначение имени устройства**

Для назначения имени устройства используются следующие команды:

```
configure
hostname <new-name>
```

где:

<net-name> - имя устройства

Например: изменим имя устройства на vesr124-2-1

```
vesr124-1#
vesr124-1# config
vesr124-1(config)# hostname vesr-1
vesr124-1(config)# do commit
Configuration has been successfully applied and saved to flash. Commit timer started, changes will be reverted in 600 seconds.
vesr-1(config)# do confirm
Configuration has been confirmed. Commit timer canceled.
vesr-1(config)# exit
vesr-1#
```

РИСУНОК 3-6. ЭКРАН ИЗМЕНЕНИЯ НАЗВАНИЯ УСТРОЙСТВА.

Готово!

Установка параметров подключения к публичной сети (WAN) и локальной сети (LAN)

Для настройки сетевого интерфейса маршрутизатора в публичной сети (WAN) необходимо назначить устройству параметры, определённые провайдером сети – IP-адрес, маска подсети и адрес шлюза по умолчанию. Это мы поручим сделать нашему хосту посредством включения режима DHCP клиента. Вм сетевые настройки маршрутизатор получит по запросу с сервера DHCP роутера, подключенного к сети провайдера Интернет, поскольку виртуальная сетевая карта виртуального маршрутизатора подключена в режиме моста к сетевой карте основного ПК.

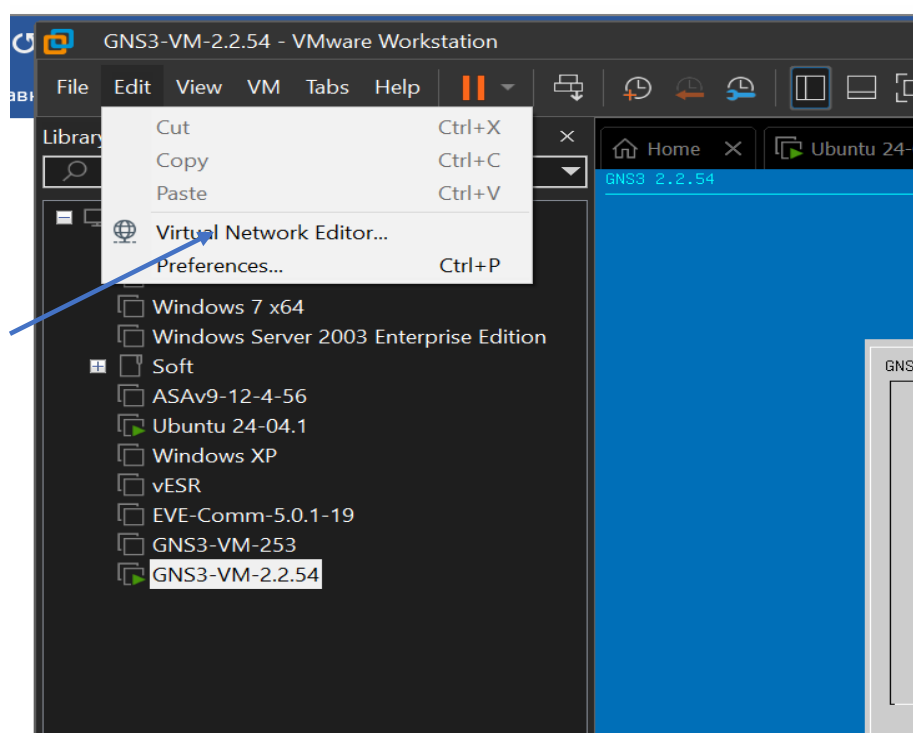


РИСУНОК 3-8. ЭКРАН НАСТРОЙКИ ВИРТУАЛЬНОЙ СЕТИ.

на пункт “Virtual Network Editor” и получаем панель управления сетевыми картами и сетями.

На этом экране необходимо выбрать пункт меню “Change Setting” и нажать на него.

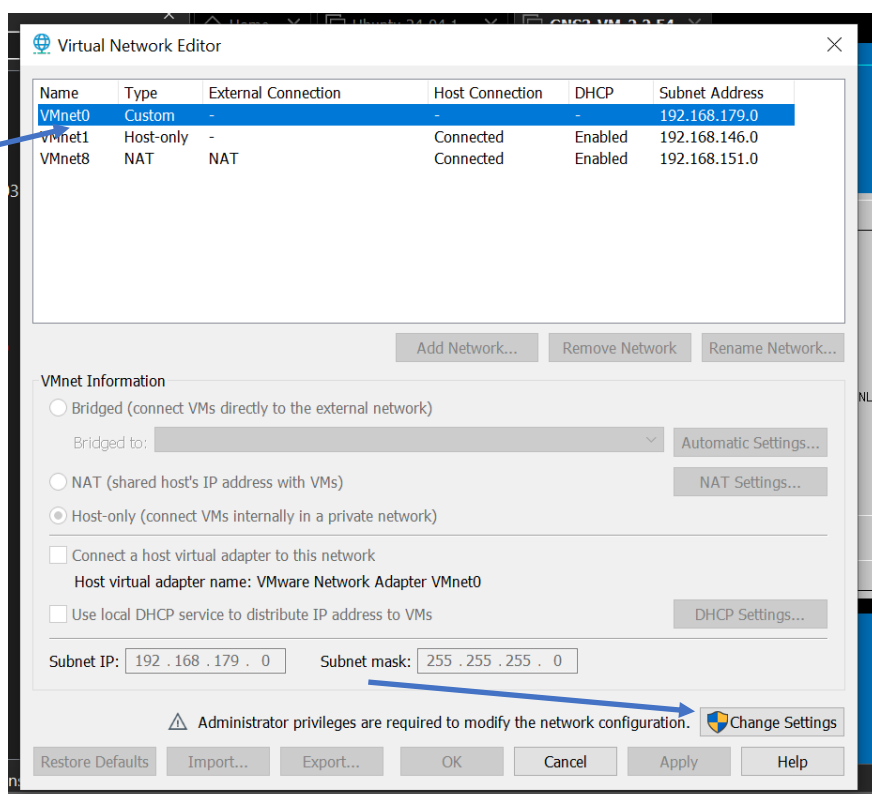


РИСУНОК 3-9. ЭКРАН ВЫБОРА СЕТЕВОГО АДАПТЕРА.

Убедитесь, что сеть VMnet0 в режиме моста (Bridged) и соединена с физической сетевой картой ПК, которая ведет к роутеру.

Лабораторные работы с виртуальным сервисным маршрутизатором vESR
В графическом симуляторе GNS3

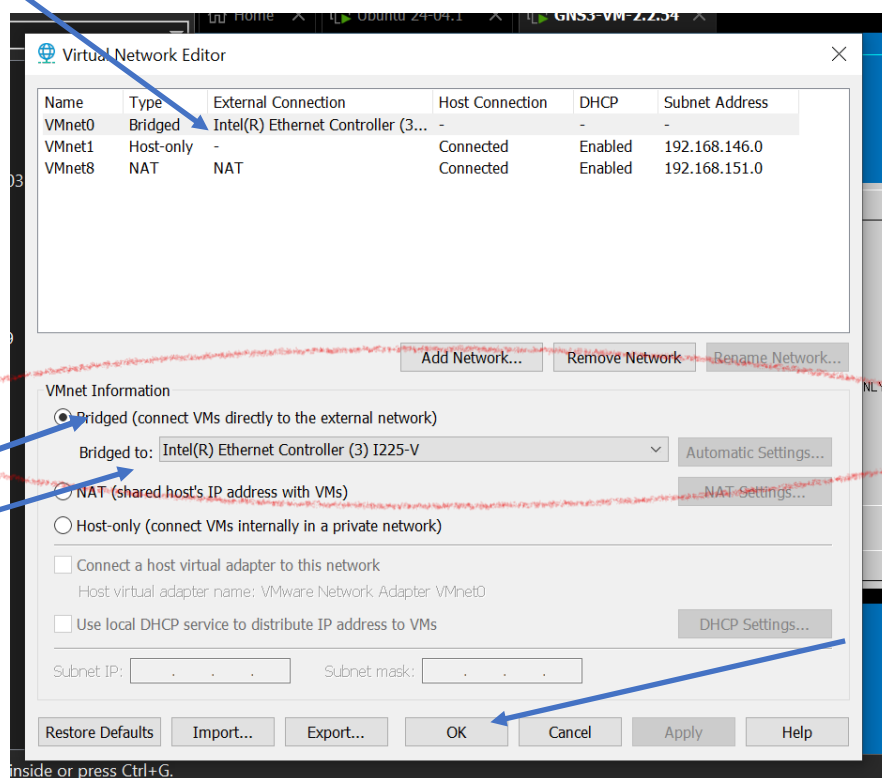


РИСУНОК 3-10. ЭКРАН ВЫБОРА ФИЗИЧЕСКОГО ПРИСОЕДИНЕНИЯ.

Например настройки автоматического получения сетевых настроек :

Для начала посмотрим какие у нас есть интерфейсы:

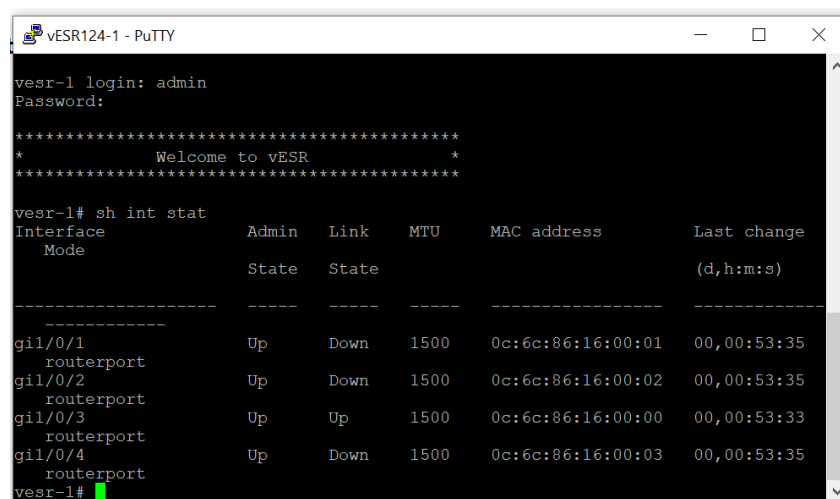


РИСУНОК 3-11. ЭКРАН СОСТОЯНИЯ СЕТЕВЫХ АДАПТЕРОВ
УСТРОЙСТВА.

Может использовать для выхода в интернет интерфейс gi1/0/1 и для внутренней сети gi1/0/2. Есть еще одна тонкость. Если посмотреть на список интерфейсов выше, то видно, что они в состоянии Down и MAC адреса не по порядку выстроены. Это ведет к не работоспособности интерфейсов. Они в состоянии Down.

Команда

vesr(debug)#nic bind auto debug

в контексте устройства vESR от Eltex означает **автоматическое назначение MAC-адресов интерфейсов** в режиме отладки (debug). docs.eltex-co.ruruits.ru

Эта команда позволяет автоматически привязать MAC-адреса доступных интерфейсов к соответствующим интерфейсам vESR, без ручного ввода данных. После выполнения команды необходимо перезагрузить устройство, чтобы изменения вступили в силу.

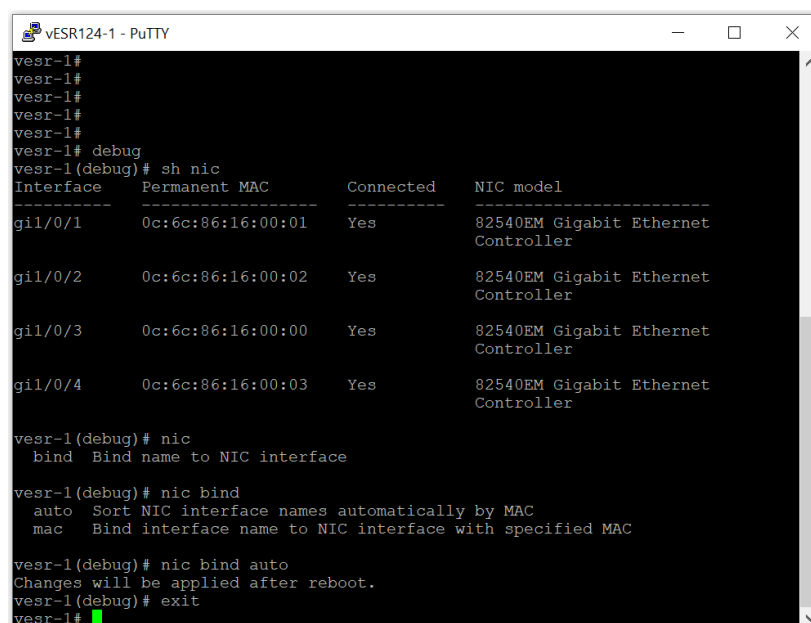
Пример использования команды:

vesr(debug)#nic bind auto

После этого в списке доступных интерфейсов (выводимом командой

vesr(debug)#show nic) будут отображаться автоматически назначенные MAC-адреса. Если нужно изменить назначение, можно скорректировать команду, указав нужный MAC-адрес вместо auto.

Лечить нужно следующими командами:



```

vESR124-1 - PuTTY
vesr-1#
vesr-1#
vesr-1#
vesr-1#
vesr-1#
vesr-1# debug
vesr-1(debug)# sh nic
Interface      Permanent MAC      Connected      NIC model
-----
gi1/0/1        0c:6c:86:16:00:01   Yes            82540EM Gigabit Ethernet Controller
gi1/0/2        0c:6c:86:16:00:02   Yes            82540EM Gigabit Ethernet Controller
gi1/0/3        0c:6c:86:16:00:00   Yes            82540EM Gigabit Ethernet Controller
gi1/0/4        0c:6c:86:16:00:03   Yes            82540EM Gigabit Ethernet Controller

vesr-1(debug)# nic
bind Bind name to NIC interface

vesr-1(debug)# nic bind
auto Sort NIC interface names automatically by MAC
mac Bind interface name to NIC interface with specified MAC

vesr-1(debug)# nic bind auto
Changes will be applied after reboot.
vesr-1(debug)# exit
vesr-1#
  
```

РИСУНОК 3-12. ЭКРАН НАСТРОЙКИ СООТВЕТСТВИЯ MAC АДРЕСОВ.

Затем нужно перезагрузить устройство командой `reboot system`. И вот теперь все хорошо с ним-MAC адреса выстроены и интерфейс к провайдеру в UP:

```
vesr124-2-1# sh int stat
```

Interface	Admin	Link	MTU	MAC address	Last change
Mode	State	State		(d,h:m:s)	
gi1/0/1	Up	Up	1500	0c:6c:86:16:00:00	00,00:01:59
gi1/0/2	Up	Down	1500	0c:6c:86:16:00:01	00,00:02:01
gi1/0/3	Up	Down	1500	0c:6c:86:16:00:02	00,00:02:01
gi1/0/4	Up	Down	1500	0c:6c:86:16:00:03	00,00:02:01

```
vesr124-2-1# config
vesr124-2-1(config)# int gi1/0/1
vesr124-2-1(config-if-gi)# description WAN
vesr124-2-1(config-if-gi)# ip address dhcp
vesr124-2-1(config-if-gi)# exit
vesr124-2-1(config)# int gi1/0/2
vesr124-2-1(config-if-gi)# description LAN
vesr124-2-1(config-if-gi)# ip address 172.16.1.1/24
vesr124-2-1(config-if-gi)# exit
vesr124-2-1(config)# do commit
Nothing to commit in configuration
vesr124-2-1(config)# do confirm
Nothing to confirm in configuration. You must commit some changes
```

first.

```
vesr124-2-1(config)# exit
vesr124-2-1#
```

Параметры интерфейса - gi1/0/1 (WAN):
IP-адрес: DHCP

Для подключения сетевых устройств внутренней сети за виртуальным маршрутизатором возьмем, например сеть 172.16.1.1/24:

Параметры интерфейса - gi1/0/2 (LAN):
IP-адрес: 172.16.1.1/24

Проверка назначения сетевых параметров:
`show interfaces description`
`show ip interfaces`

```

show ip route
vesr124-2-1# show interfaces description
Interface      Admin Link  Description
              State State
-----
gi1/0/1        Up    Up    WAN
gi1/0/2        Up    Down  LAN
gi1/0/3        Up    Down  --
gi1/0/4        Up    Down  --
vesr124-2-1# show ip interfaces
IP address      Interface      Admin Link
Type  Precedence
-----
DHCP  192.168.10.74/24      gi1/0/1        Up    Up
      172.16.1.1/24      gi1/0/2        Up    Down
static primary
vesr124-2-1# sh ip route
Codes: C - connected, S - static, R - RIP derived,
       O - OSPF derived, IA - OSPF inter area route,
       E1 - OSPF external type 1 route, E2 - OSPF external type 2
route
       B - BGP derived, D - DHCP derived, K - kernel route, V - VRRP
route
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       H - NHRP, * - FIB route

D    * 0.0.0.0/0      [40/0]      via 192.168.10.1 on gi1/0/1
[static 18:20:49]
C    * 192.168.10.0/24 [0/0]      dev gi1/0/1      [direct
18:20:49]

Проверяем связность сети между сами виртуальным
маршрутизатором и внешней сетью:
vesr124-2-1#
vesr124-2-1# ping 77.88.8.8
PING 77.88.8.8 (77.88.8.8) 56 bytes of data.
!!!!
--- 77.88.8.8 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4011ms
rtt min/avg/max/mdev = 8.124/12.859/21.669/5.021 ms
vesr124-2-1# ping cisco.com

```

PING cisco.com (72.163.4.185) 56 bytes of data.

!!!!

--- cisco.com ping statistics ---

5 packets transmitted, 5 received, 0% packet loss, time 4009ms

rtt min/avg/max/mdev = 160.928/163.197/165.601/1.983 ms

Есть дефолтный маршрут в мир и работает DNS провайдера. Всё хорошо.

Настройка проверки связности через ICMP

Изменим схему проекта и включим в него дополнительные устройства, находящиеся ха виртуальным маршрутизатором в локальной сети 172.16.1.0/24. Для этого добавим стандартный коммутатор из поставки GNS3 и эмулятор ПК.

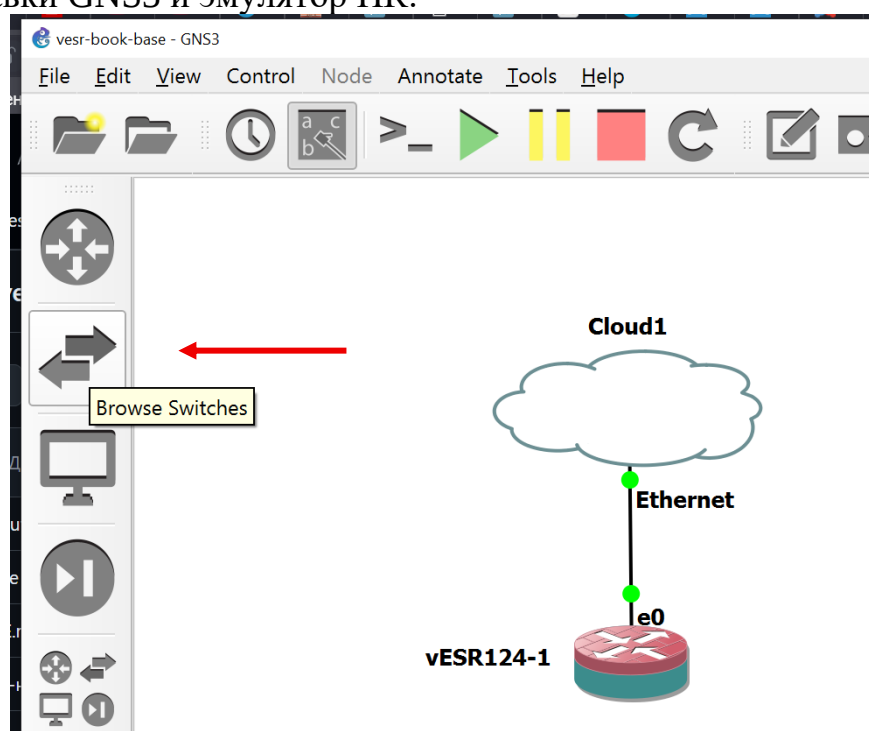


РИСУНОК 3-13. ЭКРАН ДОБАВЛЕНИЯ КОММУТАТОРА В СХЕМУ.

Мышь переводим курсор на иконку с двумя горизонтальными стрелками в левой части навигационной панели и нажимаем левую кнопку мыши. В результате получим новое окно с иконками предустановленных концентраторов и коммутаторов в GNS3. Из этого списка нужно курсором мыши выбрать иконку с надписью Ethernet Switch и зажав левую кнопку мыши перетащить иконку коммутатора на схему, расположив ее под виртуальным маршрутизатором. В появившемся окне выбора среды

Лабораторные работы с виртуальным сервисным маршрутизатором vESR
В графическом симуляторе GNS3

виртуализации выбрать имя вашего ПК (на экране будет имя вашего ПК, в отличии от рисунка), а не имя виртуальной машины GNS3) :

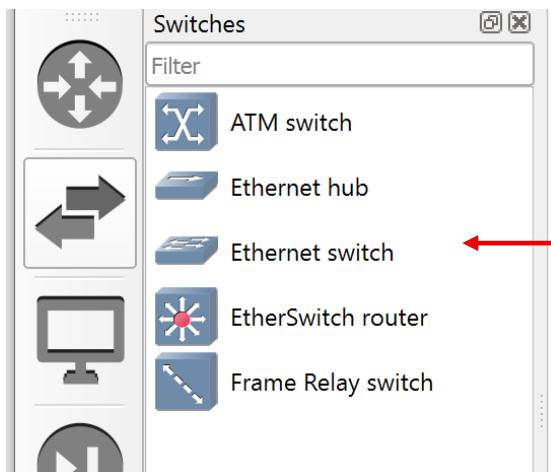


РИСУНОК 3-14. ЭКРАН ВЫБОРА КОММУТАТОРА ИЗ СПИСКА.

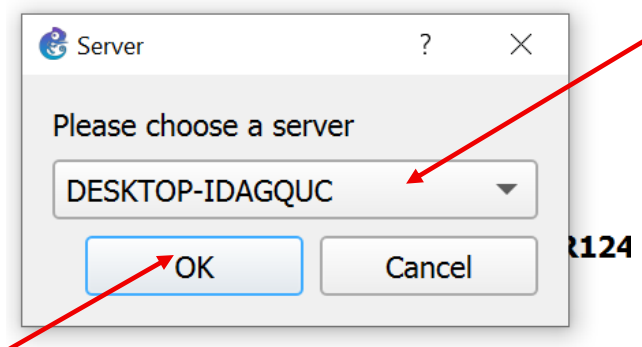


РИСУНОК 3-15. ЭКРАН ВЫБОРА МЕСТА ВИРТУАЛИЗАЦИИ.

В результате должна получиться вот такая схема:

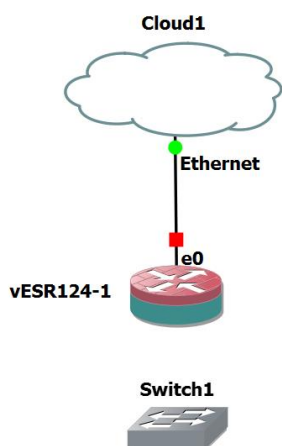


РИСУНОК 3-16. СХЕМА СОЕДИНЕНИЯ УСТРОЙСТВ.

Приступаем к подсоединению нового сетевого устройства к виртуальному маршрутизатору. Для этого переведите курсор мыши на иконку кабеля с коннектором rg45 в самой нижней части левой навигационной панели и нажмите левую кнопку мыши. На иконку кабеля появится красный кружок с белым крестиком, а курсор мыши примет вид крестика. Переведите курсор мыши на коммутатор под виртуальным маршрутизатором и нажмите левую кнопку мыши. В результате появится окно выбора имеющихся на коммутаторе сетевых интерфейсов. Выберите Ethernet 0:

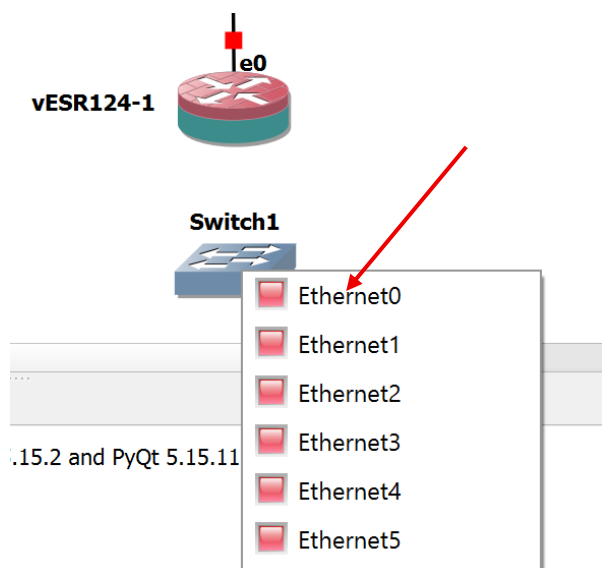


РИСУНОК 3-17. ЭКРАН ВЫБОРА ИНТЕРФЕЙСА КОММУТАТОРА.

В результате за вашим курсором в виде крестика потянется линия. Протащите ее до виртуального маршрутизатора и на нем нажмите левую клавишу мыши.

Появится окно выбора имеющихся сетевых интерфейсов виртуального маршрутизатора. Снова левой клавишей мыши выберите Ethernet1:

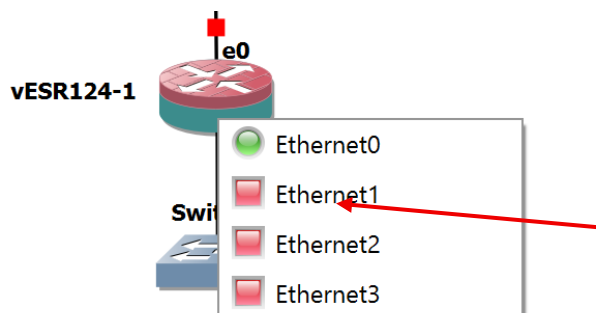


РИСУНОК 3-18. ЭКРАН ВЫБОРА ИНТЕРФЕЙСА МАРШРУТИЗАТОРА.

Отключите клавишей Esc режим выбора соединительных линий. И запустите все устройства нажав на иконку с большим зеленым треугольником в меню.

```
vesr124-2-1# sh int sta
```

Interface	Admin	Link	MTU	MAC address	Last change
Mode	State	State			(d,h:m:s)

```

-----
--
      gi1/0/1      Up   Up   1500  0c:6c:86:16:00:00  00,00:01:29
routerport
      gi1/0/2      Up   Up   1500  0c:6c:86:16:00:01  00,00:01:29
routerport
      gi1/0/3      Up   Down 1500  0c:6c:86:16:00:02  00,00:01:30
routerport
      gi1/0/4      Up   Down 1500  0c:6c:86:16:00:03  00,00:01:30
routerport
vesr124-2-1#

```

Используя те же приёмы подключаем к нашему коммутатору эмулятор персонального компьютера.

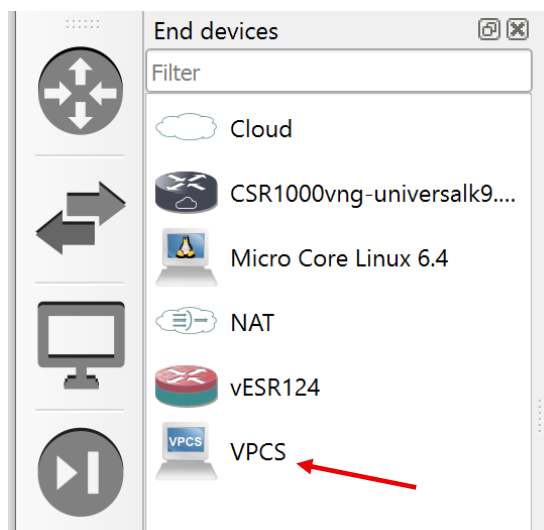


РИСУНОК 3-19. ЭКРАН ВЫБОРА ЭМУЛЯТОРА ПК.

Нажатием на левую клавишу мыши на иконке с изображением монитора в левой панели навигационного меню вызывается окно выбора конечных устройств. Нам нужно выделить устройство с названием VPCS, снова выбрать в качестве эмулятора свой ПК и перетащить на схему, расположив иконку слева от коммутатора. Следуя тем же шагам, что были применены в случае с соединением коммутатора, соединим виртуальный ПК с коммутатором, выбрав порт Ethernet1:

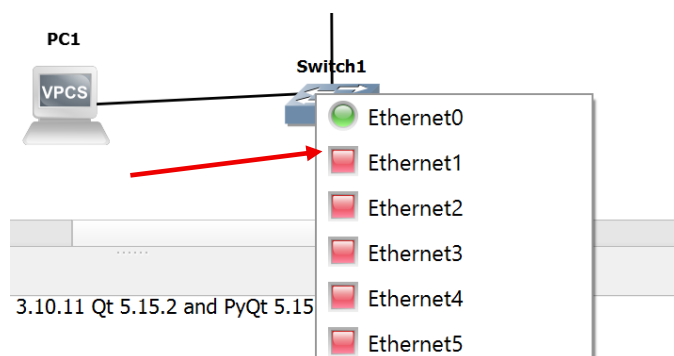


РИСУНОК 3-20. ЭКРАН ВЫБОРА ИНТЕРФЕЙСА КОММУТАТОРА.

Необходимо провести первоначальную настройку для удобства в дальнейшей работе с виртуальным ПК. Для этого наводим курсор на иконку этого VPCS, нажимаем правую клавишу мыши, выбираем из появившегося меню верхнюю строчку с надписью Configure, нажимаем на нее, в появившемся новом окне ставим галку в пункте Auto Start Console, жмем ОК. Далее стартуем это ПК снова повторив вызов меню, но уже нажав на зеленый треугольник с надписью Start. Если при старте эмулятора ПК появится надпись, что 80 порт занят-попробуйте сделать Reload из его меню.

Для сетевых настроек возьмем следующие значения:

IP address 172.16.1.10

Gateway 172.16.1.1

DNS 8.8.8.8

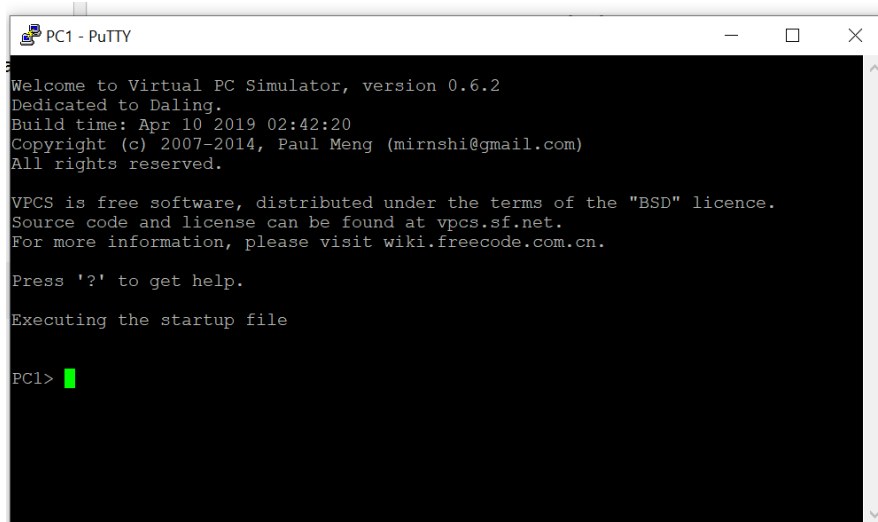


РИСУНОК 3-21. ЭКРАН ЗАГРУЗКИ ВИРТУАЛЬНОГО ЭМУЛЯТОРА ПК.

```
PC1> ip 172.16.1.10 172.16.1.1
Checking for duplicate address...
PC1 : 172.16.1.10 255.255.255.0 gateway 172.16.1.1
PC1> ip dns 8.8.8.8
PC1> save PC1
Saving startup configuration to PC1.vpc
. done
PC1>
```

Настройки сохранили , чтобы при перезагрузках не терялись сетевые настройки.

Рекомендуется для надежности все же перечитывать после старта файл PC1:

```
PC1> load PC1
Executing the file "PC1"
Checking for duplicate address...
PC1 : 172.16.1.10 255.255.255.0 gateway 172.16.1.1
PC1> sh ip
NAME      : PC1[1]
IP/MASK    : 172.16.1.10/24
GATEWAY    : 172.16.1.1
DNS       : 8.8.8.8
MAC       : 00:50:79:66:68:00
LPORT     : 13004
RHOST:PORT : 127.0.0.1:13005
MTU:      : 1500
```

Проверяем доступность маршрутизатора:

```
PC1> ping 172.16.1.1
172.16.1.1 icmp_seq=1 timeout
172.16.1.1 icmp_seq=2 timeout
172.16.1.1 icmp_seq=3 timeout
172.16.1.1 icmp_seq=4 timeout
172.16.1.1 icmp_seq=5 timeout
```

Не работает, поскольку наш виртуальный маршрутизатор изначально содержит так называемый Firewall или МэжСетевойЭкран и он не пропускает через себя никакие пакеты.

Firewall – комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами.

Из коробки firewall - включён, но не содержит никаких правил, а значит ничего и не разрешает

Порядок обработки трафика терминируемого (направленного непосредственно на сам маршрутизатор, но не через его интерфейсы) на маршрутизаторе:

Трафик проверяется правилами zone-pair any self. Если трафик не попал ни под одно из правил текущей zone-pair, переходим к следующему шагу

Трафик проверяется правилами zone-pair src-zone-name self. Если трафик не попал ни под одно из правил текущей zone-pair, он отбрасывается.

Каждая команда «match» может содержать ключ «not». При использовании данного ключа под правило будут подпадать пакеты, не удовлетворяющие заданному критерию.

На маршрутизаторе всегда существует зона безопасности с именем «self». Если в качестве получателя трафика выступает сам маршрутизатор, то есть трафик не является транзитным, то в качестве параметра указывается зона «self»

Для того чтобы маршрутизатор начал отвечать на ICMP-запросы из зоны «LAN»:

Создание зоны безопасности:

```
security zone <NAME_ZONE>
```

```
exit
```

Добавление интерфейса в зону безопасности:

```
interface <№_INT>
```

```
security-zone <NAME_ZONE>
```

```
exit
```

Например:

Создадим две зоны - "TRUSTED" для интерфейса смотрящего в LAN, и зону "UNTRUSTED" для интерфейса смотрящего в WAN

поместим соответствующие интерфейсы в зоны:

```
vesr124-2-1# config
```

```
vesr124-2-1(config)# security zone TRUSTED
```

```
vesr124-2-1(config-security-zone)# exit
```

```
vesr124-2-1(config)# security zone UNTRUSTED
```

```
vesr124-2-1(config-security-zone)# exit
```

```
vesr124-2-1(config)# interface gi1/0/1
```

```
vesr124-2-1(config-if-gi)# security-zone UNTRUSTED
```

```
vesr124-2-1(config-if-gi)# exit
```

```
vesr124-2-1(config)# interface gi1/0/2
```

```
vesr124-2-1(config-if-gi)# security-zone TRUSTED
```

```
vesr124-2-1(config-if-gi)# exit
```

```
vesr124-2-1(config)# do commit
```

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

```
vesr124-2-1(config)# do confirm
```

Configuration has been confirmed. Commit timer canceled.

```
vesr124-2-1(config)# exit
```

```
vesr124-2-1#
```

Для применения настроек:

```
do commit
```

```
do confirm
```

Проверка:

```
show security zone
```

```
vesr124-2-1# show interfaces description
```

Interface	Description	Admin	Link	State
gi1/0/1	Up	Up	WAN	
gi1/0/2	Up	Up	LAN	
gi1/0/3	Up	Down	--	
gi1/0/4	Up	Down	--	

State

gi1/0/1	Up	Up	WAN
gi1/0/2	Up	Up	LAN
gi1/0/3	Up	Down	--
gi1/0/4	Up	Down	--

```
vesr124-2-1# show security zone
```

Zone name	Interfaces
TRUSTED	gi1/0/2
UNTRUSTED	gi1/0/1

Для настройки правил зон безопасности потребуется создать профиль адресов сети «LAN», включающий адреса, которым разрешен доступ к маршрутизатору:

Создание профиля адресов сети:

```
object-group network <NAME_PROFILE>
```

```
ip address-range <IP_RANGE | IP_ADDRESS>
```

```
exit
```

где:

<NAME_PROFILE> - имя профиля адресов сети

<IP_RANGE | IP_ADDRESS> - диапазон IP-адресов записанный через "-" (дефис) или IP-адрес

Например:

создадим профиль "LAN" в котором укажем IP-адрес маршрутизатора интерфейса, который смотрит в LAN;

создадим профиль "LAN_GATEWAY" в котором укажем диапазон IP-адресов из сети LAN

```

vesr124-2-1# config
vesr124-2-1(config)# object-group network LAN
vesr124-2-1(config-object-group-network)# ip address-range 172.16.1.1
vesr124-2-1(config-object-group-network)# exit
vesr124-2-1(config)# object-group network LAN_GATEWAY
vesr124-2-1(config-object-group-network)# ip address-range 172.16.1.1-
172.16.1.254
vesr124-2-1(config-object-group-network)# exit
vesr124-2-1(config)#

```

Добавим правило, разрешающее проходить ICMP-трафику между маршрутизатором и клиентами, для того чтобы маршрутизатор начал отвечать на ICMP-запросы из зоны «TRUSTED». То есть из локальной сети (LAN)

Создадим пару зон для трафика, идущего из зоны «TRUSTED» в зону «self»

```

Действие правил разрешается командой enable
vesr124-2-1(config)# security zone-pair TRUSTED self
vesr124-2-1(config-security-zone-pair)# rule 1
vesr124-2-1(config-security-zone-pair-rule)# action permit
vesr124-2-1(config-security-zone-pair-rule)# match protocol icmp
vesr124-2-1(config-security-zone-pair-rule)# match destination-address
object-group
LAN
vesr124-2-1(config-security-zone-pair-rule)# match destination-address
object-group
vesr124-2-1(config-security-zone-pair-rule)# match destination-address
object-group
LAN_GATEWAY
vesr124-2-1(config-security-zone-pair-rule)# enable
vesr124-2-1(config-security-zone-pair-rule)# exit
vesr124-2-1(config-security-zone-pair)# exit
vesr124-2-1(config)#

```

где:

<**destination-address**> - ссылается на профиль адресов сети "LAN", в котором указан IP-адрес маршрутизатора;

<**source-address**> - ссылается на профиль адресов сети "LAN_GATEWAY", в котором указан диапазон IP-адресов сети LAN;

Для применения настроек:

do commit

do confirm

Проверка:

```
show security zone-pair configuration TRUSTED self
vesr124-2-1# show security zone-pair configuration TRUSTED self
Order:                1
Description:          --
Matching pattern:
  Protocol:            ICMP(1)
  Fragment:
  IP options:
  Source MAC:          any
  Destination MAC:     any
  ICMP type:           any
  ICMP code:           any
  Source address:      any
  Destination address: 172.16.1.1-172.16.1.254
  Destination NAT:     --
  Application:         --
Action:               Permit
Status:               Enabled
```

```
-----
vesr124-2-1#
Проверка связности с клиента из сети LAN с маршрутизатором:
vesr124-2-1# ping 172.16.1.1
PING 172.16.1.1 (172.16.1.1) 56 bytes of data.
!!!!
--- 172.16.1.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 0.074/0.218/0.623/0.208 ms
vesr124-2-1# ping 77.88.8.8
PING 77.88.8.8 (77.88.8.8) 56 bytes of data.
!!!!
--- 77.88.8.8 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 9.474/10.558/13.448/1.462 ms
vesr124-2-1# ping cisco.com
PING cisco.com (72.163.4.185) 56 bytes of data.
!!!!
--- cisco.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4013ms
rtt min/avg/max/mdev = 160.518/161.769/164.574/1.562 ms
vesr124-2-1#
```

Базовые настройки завершены.

Совет как включить протокол вывода при старте системы:

```
vesr124-2-1login: admin
```

```
Password:eve
```

```
*****
```

```
*           Welcome to vESR           *
```

```
*****
```

```
vesr124-2-1# config
```

```
vesr124-2-1(config)# syslog console
```

```
vesr124-2-1(config-syslog-console)# virtual-terminal
```

```
vesr124-2-1(config-syslog-console)# exit
```

```
vesr124-2-1(config)# do commit
```

```
vesr124-2-1(config)# do confirm
```

```
vesr124-2-1(config)# exit
```

```
vesr124-2-1#reboot system
```

После перезагрузки можно будет видеть сообщения о ходе загрузки системы. В том числе диагностические или критические для последующего исследования причин краха.

ВЫВОДЫ ПО ГЛАВЕ

- Создан проект для работы с устройством
- Создание новых пользователей
- Изменение название устройства
- Установка параметров подключения к публичной сети (WAN) и локальной сети (LAN)
- Настройка связности сети
- Что такое межсетевой экран и понятие зон безопасности

В следующей главе вы узнаете что такое протокол DHCP и как он настраивается в маршрутизаторе.

Глава 4. Настройка сервера DHCP в маршрутизаторе vESR.

Цель этой работы:

Знакомство с работой протокола и настройка сервера DHCP на маршрутизаторе.

Что такое DHCP? DHCP (Dynamic Host Configuration Protocol) — это сетевой протокол, который автоматически назначает IP-адреса и другие сетевые параметры устройствам в сети.

Основная задача DHCP — упростить управление сетью, избавив администраторов от необходимости вручную настраивать IP-адреса для каждого устройства.

DHCP Dynamic Host Configuration Protocol

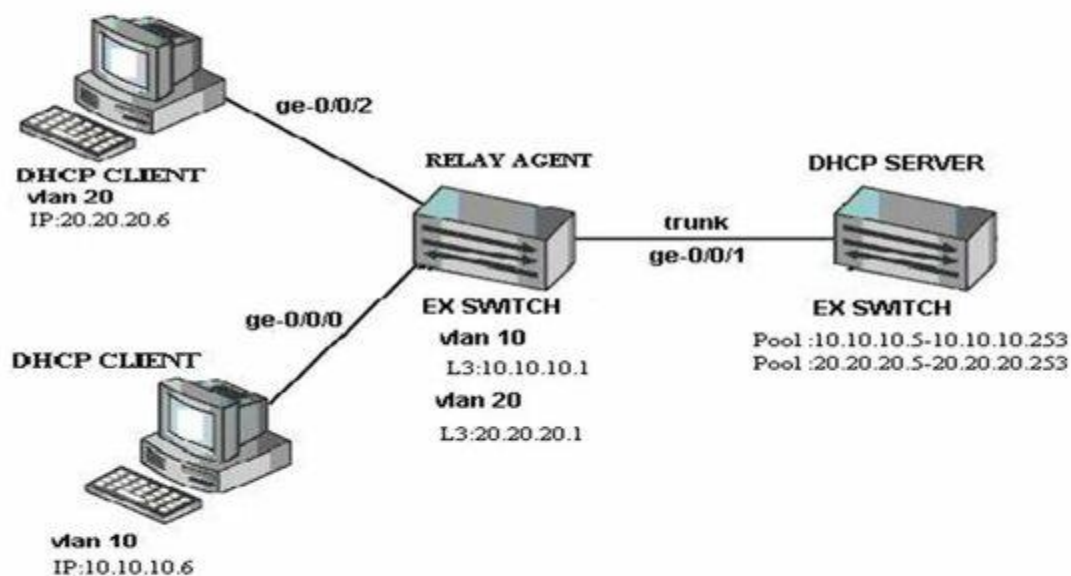


Рисунок 4-1. Схема с сервером dhcp в локальной сети.

- Принцип работы DHCP

Работа DHCP основана на взаимодействии между DHCP-клиентом (устройство, подключающееся к сети) и DHCP-сервером (устройство или сервис, управляющий распределением IP-адресов).

Процесс состоит из четырёх основных этапов:

DHCP Discover (Обнаружение). Устройство отправляет широковещательный запрос, пытаясь найти DHCP-сервер.

DHCP Offer (Предложение). Сервер отвечает пакетом DHCP Offer, предлагая свободный IP-адрес из своего пула адресов вместе с другими сетевыми параметрами.

DHCP Request (Запрос). Клиент получает предложение и отвечает серверу сообщением DHCP Request, подтверждая готовность принять предложенные параметры.

DHCP Acknowledgment (Подтверждение). Сервер подтверждает назначение IP-адреса и отправляет клиенту окончательные параметры. После этого устройство может полноценно работать в сети.

- Преимущества и недостатки

Преимущества DHCP:

автоматизация настройки сетевых параметров; ServerGate.rumksegment.ru

предотвращение конфликтов IP-адресов; help.sweb.rumksegment.ru
снижение нагрузки на сеть за счёт использования временных IP-адресов.

Недостатки DHCP:

если DHCP-сервер выходит из строя, новые устройства не смогут получить IP-адреса и подключиться к сети;

DHCP-сообщения передаются в незашифрованном виде, что делает их уязвимыми для атак;

злоумышленник может настроить несанкционированный DHCP-сервер, который будет выдавать ложные IP-адреса.

Где используется

DHCP применяется в различных типах сетей — в домашних и корпоративных. Некоторые устройства, которые используют DHCP:

компьютеры и ноутбуки;

смартфоны и планшеты;

умные устройства (камеры наблюдения, термостаты, холодильники);

сетевое оборудование (маршрутизаторы, коммутаторы).

- Настройка сервера DHCP

Добавим в нашу схему еще один виртуальный персональный компьютер, используя методы, описанные в предыдущей главе.

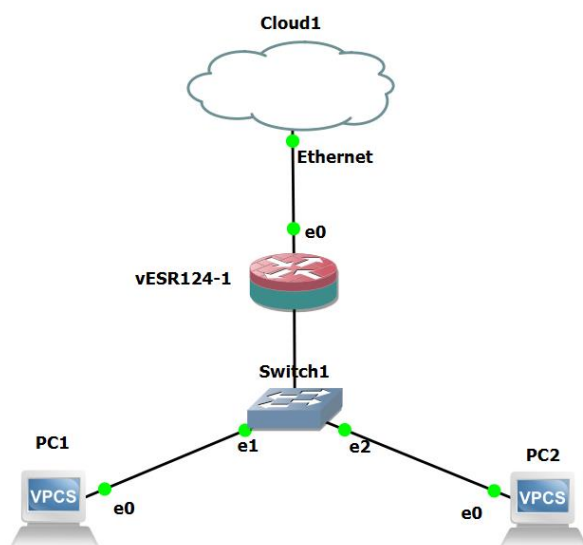


Рисунок 4-2

Нам нужно настроить работу DHCP-сервера на базе виртуального маршрутизатора vesr124-2-1. Задать пул IP-адресов из подсети 172.16.1.0/24 для раздачи клиентам. Для PC1 зарезервировать выдачу следующего IP-адреса 172.16.1.100, а для PC2 зарезервировать выдачу следующего IP-адреса 172.16.1.200, а и задать время аренды адресов 3 дня. Настроить передачу клиентам маршрута по умолчанию, доменного имени и адресов DNS-серверов с помощью DHCP-опций.

Назначаем IP-адреса на интерфейсы:

Выполняемые команды в консоли виртуального маршрутизатора vesr124-2-1:

```
configure
```

на интерфейс смотрящий в сторону глобальной сети получаем сетевые параметры по DHCP

```
interface gi1/0/1
```

```
description connection_WAN
```

```
ip address dhcp
```

```
exit
```

на интерфейс смотрящий в сторону rtr1 и rtr2 назначаем статический адрес из подсети 172.16.1.1/24

```
interface gi1/0/2
```

```
description connection_LAN
```

```
ip address 172.16.1.1/24
```

```
exit
```

Создадим зону безопасности «**TRUSTED**» и установим принадлежность интерфейса **gi1/0/2** (смотрящего в подсеть rtr1 и rtr2) такими командами:

```
security zone TRUSTED
```

```

exit
interface gi1/0/2
security-zone TRUSTED
exit
do commit
do confirm
Вывод текущего конфига из консоли vesr124-2-1:
vesr124-2-1# sh running-config
hostname vesr124-2-1
object-group network LAN
ip address-range 172.16.1.1
exit
object-group network LAN_GATEWAY
ip address-range 172.16.1.1-172.16.1.254
exit
syslog max-files 3
syslog file-size 512
syslog file tmpsys:syslog/default
severity info
exit
syslog console
virtual-serial
exit
username admin
password encrypted
$6$1jB3DT6zH05CQ7$WqbKGSvl/35jvx.NKDc6R5NpD5uy2623zfbWAO
TPhNOQgnR.zXxQzlgYwESdbOXSyhPPNojy0Q0.pMvR6Ld/
exit
username rinat
password encrypted
$6$1wbeF/CqjcFAJrob$thjkqaTLACQVWN1bRbqzFUbO5VL24jbWHbLD2Z
OXbphb.CoI7n8k3rj3j1x79RDqOLDfj2IAnECPPYIR4tmci1
privilege 15
exit
domain lookup enable
security zone TRUSTED
exit
security zone UNTRUSTED
exit

interface gigabitethernet 1/0/1
description "WAN"

```

```
security-zone UNTRUSTED
ip address dhcp
exit
interface gigabitethernet 1/0/2
description "LAN"
security-zone TRUSTED
ip address 172.16.1.1/24
exit

security zone-pair TRUSTED self
rule 1
action permit
match protocol icmp
match destination-address object-group LAN_GATEWAY
enable
exit
exit

security passwords default-expired

ip ssh server

ntp enable
ntp broadcast-client enable

licence-manager
host address elm.eltex-co.ru
exit
```

```
vesr124-2-1#
```

Прмечание: эти шаги мы уже сделали в предыдущей главе- смотри Рис. Введенные команды в тексте выведенного конфига выделены цветом и обведены рамкой.

Создадим пул адресов с именем «COMPANY» и добавим в данный пул адресов диапазон IP-адресов для выдачи в аренду клиентам сервера. Укажем параметры подсети, к которой принадлежит данный пул, и время аренды для выдаваемых адресов выполнив команды:

```
config
ip dhcp-server pool COMPANY
network 172.16.1.0/24
default-lease-time 3:00:00
address-range 172.16.1.1-172.16.1.254
```

```

        excluded-address-range 172.16.1.1          # исключаем первый
адрес из выдачи
        excluded-address-range 172.16.1254         # исключаем
последний адрес из выдачи
        address 172.16.1.100 mac-address 00:50:79:66:68:00 # MAC-адрес
PC1
        address 172.16.1.200 mac-address 00:50:79:66:68:01 # MAC-адрес
PC2
        default-router 172.16.1.1                  # в качестве шлюза будет
выдан IP-адрес интерфейса gi1/0/2
        default-server 77.88.8.8                   # в качестве DNS-сервера
будет выдан IP-адрес 77.88.8.8
        exit
        do commit
        do confirm
esr-1# config
vesr124-2-1(config)# ip dhcp-server pool COMPANY
vesr124-2-1(config-dhcp-server)# network 172.16.1.0/24
vesr124-2-1(config-dhcp-server)# default-lease-time 3:00:00
vesr124-2-1(config-dhcp-server)# address-range 172.16.1.1-
172.16.1.254
vesr124-2-1(config-dhcp-server)# excluded-address-range 172.16.1.1
vesr124-2-1(config-dhcp-server)# excluded-address-range 172.16.1.254
vesr124-2-1(config-dhcp-server)# address 172.16.1.100 mac-address
00:50:79:66:68:00
vesr124-2-1(config-dhcp-server)# address 172.16.1.200 mac-address
00:50:79:66:68:01
vesr124-2-1(config-dhcp-server)# default-router 172.16.1.1
vesr124-2-1(config-dhcp-server)# dns-server 77.88.8.8
vesr124-2-1(config-dhcp-server)# exit
vesr124-2-1(config)# do commit
Configuration has been successfully applied and saved to flash. Commit
timer started, changes will be reverted in 600 seconds.
2025-05-29T18:28:39+00:00 %CLI-I-CRIT: user admin from console
input: do commit
vesr124-2-1(config)# do confirm
Configuration has been confirmed. Commit timer canceled.
2025-05-29T18:28:44+00:00 %CLI-I-CRIT: user admin from console
input: do confirm
vesr124-2-1(config)# exit
vesr124-2-1#

```

MAC адреса виртуальных ПУ нужно взять дав команды `sh ip` и скопировав значения MAC адресов консолях этих ПКБ благо это делается простым вырезанием курсором мыши и нажатием сочетаний клавиш `Ctrl+Insert`, вставка в окно терминала соответственно `Shift+Insert` :

```
PC1> sh ip
NAME      : PC1[1]
IP/MASK    : 0.0.0.0/0
GATEWAY    : 0.0.0.0
DNS        :
MAC      : 00:50:79:66:68:00
LPORT     : 13006
RHOST:PORT : 127.0.0.1:13007
MTU:       : 1500
```

```
PC2> sh ip
NAME      : PC2[1]
IP/MASK    : 0.0.0.0/0
GATEWAY    : 0.0.0.0
DNS        :
MAC      : 00:50:79:66:68:01
LPORT     : 13008
RHOST:PORT : 127.0.0.1:13009
MTU:       : 1500
```

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 :

```
config
object-group service dhcp_server
port-range 67
exit
object-group service dhcp_client
port-range 68
exit
do commit
do confirm
do show running-config
```

Протокол работы в консоли в режиме конфигурации:

```
vesr124-2-1(config)# object-group service dhcp_service
vesr124-2-1(config-object-group-service)# port-range 67
vesr124-2-1(config-object-group-service)# exit
vesr124-2-1(config)# object-group service dhcp_client
vesr124-2-1(config-object-group-service)# port-range 68
vesr124-2-1(config-object-group-service)# exit
vesr124-2-1(config)# do commit
```

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

2025-05-29T18:47:10+00:00 %CLI-I-CRIT: user admin from console

input: do commit

```
vesr124-2-1(config)# do confirm
```

Configuration has been confirmed. Commit timer canceled.

2025-05-29T18:47:15+00:00 %CLI-I-CRIT: user admin from console

input: do confirm

```
vesr124-2-1(config)# do show running-config
```

```
hostname vesr124-2-1
```

```
object-group service dhcp_service
```

```
port-range 67
```

```
exit
```

```
object-group service dhcp_client
```

```
port-range 68
```

```
exit
```

У нас уже ранее в предыдущей главе было создано одно правило для пропуска пингов файрволом.

```
security zone-pair TRUSTED self
```

```
rule 1
```

```
action permit
```

```
match protocol icmp
```

```
match destination-address object-group LAN_GATEWAY
```

```
enable
```

Теперь нужно добавить еще одно для пропуска пакетов протокола DHCP:

```
config
```

```
security zone-pair TRUSTED self
```

```
rule 2
```

```
match protocol udp
```

```
match source-port dhcp_client
```

```
match destination-port dhcp_server
```

```
action permit
```

```

enable
exit
exit

vesr124-2-1# config
vesr124-2-1(config)# security zone-pair TRUSTED self
vesr124-2-1(config-security-zone-pair)# rule 2
vesr124-2-1(config-security-zone-pair-rule)# match protocol udp
vesr124-2-1(config-security-zone-pair-rule)# match source-port object-
group dhcp_client
vesr124-2-1(config-security-zone-pair-rule)# match destination-port
object-group dhcp_service
vesr124-2-1(config-security-zone-pair-rule)# action permit
vesr124-2-1(config-security-zone-pair-rule)# enable
vesr124-2-1(config-security-zone-pair-rule)# exit
vesr124-2-1(config-security-zone-pair)# exit
vesr124-2-1(config)# exit
Warning: you have uncommitted configuration changes.
vesr124-2-1# commit
Configuration has been successfully applied and saved to flash. Commit
timer started, changes will be reverted in 600 seconds.
2025-05-29T19:00:58+00:00 %CLI-I-CRIT: user admin from console
input: commit
vesr124-2-1# confirm
Configuration has been confirmed. Commit timer canceled.
2025-05-29T19:01:01+00:00 %CLI-I-CRIT: user admin from console
input: confirm
vesr124-2-1#
Разрешим работу сервера:
vesr124-2-1# config
vesr124-2-1(config)# ip dhcp-server
vesr124-2-1(config)# do commit
Configuration has been successfully applied and saved to flash. Commit
timer started, changes will be reverted in 600 seconds.
2025-05-29T19:04:10+00:00 %CLI-I-CRIT: user admin from console
input: do commi
vesr124-2-1(config)# do confirm
Configuration has been confirmed. Commit timer canceled.
2025-05-29T19:04:22+00:00 %CLI-I-CRIT: user admin from console
input: do confim
vesr124-2-1(config)# exit
vesr124-2-1#

```

Включаем на PC1 и 3C2 автоматическое получение сетевых настроек по DHCP:

```
PC1> ip dhcp
DORA IP 172.16.1.100/24 GW 172.16.1.1
PC1> save PC1
Saving startup configuration to PC1.vpc
. done
```

```
PC2> ip dhcp
DORA IP 172.16.1.200/24 GW 172.16.1.1
PC2> save PC2
Saving startup configuration to PC2.vpc
. done
```

Проверяем параметры DHCP-сервера:

```
show ip dhcp server pool COMPANY
vesr124-2-1# show ip dhcp server pool COMPANY
Name:                COMPANY
Network:              172.16.1.0/24
Address-ranges:       172.16.1.1-172.16.1.254
Excluded-address-ranges: 172.16.1.1
                      172.16.1.254
Addresses:            172.16.1.100 00:50:79:66:68:00
                      172.16.1.200 00:50:79:66:68:01
Default-router:       172.16.1.1
Dns-server:           77.88.8.8
Max lease time (d:h:m): 001:00:00
Default lease time (d:h:m): 003:00:00
Адреса выдаются. И интерфейс маршрутизатора доступен:
PC2> ping 172.16.1.1
84 bytes from 172.16.1.1 icmp_seq=1 ttl=64 time=4.332 ms
84 bytes from 172.16.1.1 icmp_seq=2 ttl=64 time=1.772 ms
84 bytes from 172.16.1.1 icmp_seq=3 ttl=64 time=3.388 ms
84 bytes from 172.16.1.1 icmp_seq=4 ttl=64 time=3.552 ms
84 bytes from 172.16.1.1 icmp_seq=5 ttl=64 time=2.479 ms
```

ВЫВОДЫ ПО ГЛАВЕ

- Принцип работы протокола DHCP
- Преимущества и недостатки
- Настройка сервера DHCP
- Проверка работы сервера

Как результат работы получена рабочая схема с сервером DHCP и клиентами локальной сети, автоматически получающие сетевые адреса.

В следующей главе вы узнаете как настроить доступ в сеть интернет из локальной сети

Глава 5. Настройка NAT(SNAT) для доступа в Интернет в виртуальном маршрутизаторе vESR.

Цель работы:

Дать выход в Интернет клиентам локальной сети. Эти клиенты автоматически получили сетевыми адреса из не маршрутизируемых блоков сетей в Интернет и не могут выйти во внешний мир. Решается эта задача трансляцией сетевых адресов в так называемые «белые» адреса, которые могут использоваться для выхода в интернет через провайдера.

NAT (Network Address Translation) — это механизм преобразования локальных (частных) IP-адресов в глобальные (публичные) и наоборот. Функция Source NAT (SNAT) используется для подмены адреса источника у пакетов, проходящих через сетевой шлюз и обеспечивает безопасность сети.

- Процесс работы NAT:

Устройство отправляет запрос в интернет. Оно использует внутренний IP-адрес, который уникален только внутри локальной сети.

Когда пакет данных достигает маршрутизатора, NAT заменяет внутренний IP-адрес на внешний IP-адрес маршрутизатора. При этом маршрутизатор запоминает, какой внутренний IP-адрес связан с каким внешним IP-адресом и портом.

Когда ответ от сервера приходит обратно в сеть, маршрутизатор использует свои таблицы NAT, чтобы направить пакет данных к правильному устройству в локальной сети, заменяя внешний IP-адрес обратно на внутренний.

Типы NAT

Существует несколько типов NAT:

Статический NAT (Static NAT). Создаёт постоянное соответствие между внутренним и внешним IP-адресами. Обычно используется для серверов, которые должны быть доступными из внешнего интернета, например, веб-серверов или почтовых серверов.

Динамический NAT (Dynamic NAT). Присваивает внутренним IP-адресам временные внешние IP-адреса из пула доступных адресов. Это позволяет множеству устройств в локальной сети использовать один внешний IP-адрес, но при этом адреса могут изменяться.

PAT (Port Address Translation), также известный как NAT Overload. Позволяет множеству устройств использовать один внешний IP-адрес, отличая их по номерам портов. Это наиболее распространённый тип NAT.

- Преимущества и недостатки NAT

Преимущества NAT:

Экономия IP-адресов. NAT позволяет сократить потребность в публичных IP-адресах, так как несколько устройств в локальной сети могут использовать один и тот же публичный IP-адрес.

Повышение безопасности. NAT скрывает внутреннюю структуру сети от внешних пользователей, что затрудняет несанкционированный доступ извне.

Управление трафиком. NAT помогает управлять трафиком, направляя запросы к правильным устройствам в локальной сети.

Недостатки NAT:

Задержки в пути из-за преобразования. Каждый сетевой пакет, покидающий локальную сеть и направляющийся в Интернет, должен пройти процесс перевода адресов на граничном маршрутизаторе.

Некоторые приложения не функционируют при включённом NAT. Например, приложения, которые применяют передачу данных с использованием определённых портов или требуют прямого взаимодействия с уникальными IP-адресами.

Сложности с туннелированием протоколов, таких как IPsec. NAT изменяет заголовки пакетов, а это может привести к проблемам с корректной передачей зашифрованных данных.

Используем схему подключения сетевых устройств, рассмотренную в предыдущей главе для настройки доступа с PC1 (172.16.1.100/24) и PC2 (172.16.1.200/24) к публичной сети с использованием функции Source NAT, через IP-адрес виртуальный маршрутизатор vesr124-2-1 который смотрит в настоящую сеть Интернет. Работу по настройке интерфейсов, назначение адресов и межсетевого экрана мы уже проделали в предыдущей главе, но сказано неоднократно было: «Повторение-мать учения», поэтому не будет нарушать традицию (вводить снова эти команды в консоли маршрутизатора не обязательно):

Проверяем доступ к сети с устройства PC2:

```
PC2> ping 8.8.8.8
8.8.8.8 icmp_seq=1 timeout
8.8.8.8 icmp_seq=2 timeout
8.8.8.8 icmp_seq=3 timeout
8.8.8.8 icmp_seq=4 timeout
8.8.8.8 icmp_seq=5 timeout
```

Назначаем IP-адреса на интерфейсы командами:

```
configure
```

на интерфейс смотрящий в сторону глобальной сети получаем сетевые параметры по DHCP

```
interface gi1/0/1
description connection_WAN
ip address dhcp
```

```
exit
```

на интерфейс смотрящий в сторону PC1 и PC2 назначаем статический адрес из подсети 172.16.1.0/24

```
interface gi1/0/2
description connection_LAN_GATEWAY
ip address 172.16.1.1/24
exit
```

Создадим зону безопасности «**TRUSTED**» и установим принадлежность интерфейса **gi1/0/2** (смотрящего в подсеть PC1 и PC2) командами:

```
security zone TRUSTED
exit
interface gi1/0/2
security-zone TRUSTED
exit
```

Создадим зону безопасности «**unTRUSTED**» и установим принадлежность интерфейса **gi1/0/1** (смотрящего в настоящую сеть Интернет) командами:

```
security zone UNTRUSTED
exit
interface gi1/0/1
security-zone UNTRUSTED
exit
do commit
```

Для конфигурирования SNAT и настройки правил зон безопасности потребуется создать профиль адресов сети «LAN_GATEWAY», включающий адреса, которым разрешен выход в публичную сеть, и профиль адреса публичной сети «WAN».

```
object-group network LAN_GATEWAY
ip address-range 172.16.1.1-172.16.1.254    # указываем всю
локальную сеть
exit
```

Вышеприведенные команды уже должны быть в конфигурационном файле виртуального маршрутизатора, поскольку мы их вводили ранее в предыдущей главе при настройке сервера DHCP. Проверить их наличие можно командой show run.

Для настройки NAT необходимо знать IP адрес интерфейса , «смотрящего» в Интернет. Для этого даем команду:

```
vesr124-2-1# sh ip interfaces gigabitethernet 1/0/1
```

Link	Type	Precedence	IP address	Interface	Adm	in
------	------	------------	------------	-----------	-----	----

```

-----
--  -----
Up  192.168.10.74/24                    gi1/0/1          Up
    DHCP    --
    И копируем IP адрес.
    А вот эту команду мы еще не вводили, открываем консоль и вводим
команды:
    configure
    object-group network WAN
    ip address-range 192.168.10.74      # IP-адрес - смотрящий в
настоящую сеть Интернет
    exit
    do commit
    do confirm
    vesr124-2-1# config
    vesr124-2-1(config)# object-group network WAN
    vesr124-2-1(config-object-group-network)# ip address-range
192.168.10.74
    vesr124-2-1(config-object-group-network)# exit
    vesr124-2-1(config)# do commit
    Configuration has been successfully applied and saved to flash. Commit
timer started, changes will be reverted in 600 seconds.
    2025-05-30T06:58:49+00:00 %CLI-I-CRIT: user admin from console
input: do commit
    vesr124-2-1(config)# do confirm
    Configuration has been confirmed. Commit timer canceled.
    2025-05-30T06:58:58+00:00 %CLI-I-CRIT: user admin from console
input: do confirm
    vesr124-2-1(config)#
    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_GATEWAY для
соблюдения ограничения на выход в публичную сеть. Действие правил
разрешается командой enable:
    security zone-pair TRUSTED UNTRUSTED
    rule 1
    match source-address LAN_GATEWAY
    action permit
    enable
    exit

```

```

exit
do commit
do confirm
vesr124-2-1(config)# security zone-pair TRUSTED UNTRUSTED
vesr124-2-1(config-security-zone-pair)# rule 1
vesr124-2-1(config-security-zone-pair-rule)# match source-address
object-group LAN_GATEWAY
vesr124-2-1(config-security-zone-pair-rule)# action permit
vesr124-2-1(config-security-zone-pair-rule)# enable
vesr124-2-1(config-security-zone-pair-rule)# exit
vesr124-2-1(config-security-zone-pair)# exit
vesr124-2-1(config)# do commit
Configuration has been successfully applied and saved to flash. Commit
timer started, changes will be reverted in 600 seconds.
2025-05-30T07:05:53+00:00 %CLI-I-CRIT: user admin from console
input: do commit
vesr124-2-1(config)# do confirm
Configuration has been confirmed. Commit timer canceled.
2025-05-30T07:05:59+00:00 %CLI-I-CRIT: user admin from console
input: do confirm
vesr124-2-1(config)#
Конфигурируем сервис SNAT. Первым шагом задаётся IP-адрес
публичной сети (WAN), используемых для сервиса SNAT:
nat source
pool WAN
ip address-range 192.168.10.74      # IP-адрес isp - смотрящий в
настоящую сеть Интернет
exit

```

Создаём набор правил SNAT. В атрибутах набора укажем, что правила применяются только для пакетов, направляющихся в публичную сеть – в зону **UNTRUSTED**. Правила включают проверку адреса источника данных на принадлежность к пулу **LAN_GATEWAY**:

```

ruleset SNAT
to zone UNTRUSTED
rule 1
match source-address LAN_GATEWAY
action source-nat pool WAN
enable
exit
exit
do commit

```

```

do confirm
vesr124-2-1(config)#
vesr124-2-1(config)# nat source
vesr124-2-1(config-snat)# pool WAN
vesr124-2-1(config-snat-pool)# ip address-range 192.168.10.74
vesr124-2-1(config-snat-pool)# exit
vesr124-2-1(config-snat)# ruleset SNAT
vesr124-2-1(config-snat-ruleset)# to zone TRUSTED
vesr124-2-1(config-snat-ruleset)# rule 1
vesr124-2-1(config-snat-rule)# match source-address object-group
LAN_GATEWAY
vesr124-2-1(config-snat-rule)# action source-nat pool WAN
vesr124-2-1(config-snat-rule)# enable
vesr124-2-1(config-snat-rule)# exit
vesr124-2-1(config-snat-ruleset)# exit
vesr124-2-1(config-snat)# exit
vesr124-2-1(config)# do commit
Configuration has been successfully applied and saved to flash. Commit
timer started, changes will be reverted in 600 seconds.
2025-05-30T07:09:54+00:00 %CLI-I-CRIT: user admin from console
input: do commit
vesr124-2-1(config)# do confirm
Configuration has been confirmed. Commit timer canceled.
2025-05-30T07:09:59+00:00 %CLI-I-CRIT: user admin from console
input: do confirm
vesr124-2-1(config)# exit
vesr124-2-1#

```

Проверяем с PC1 и PC2 доступ в Интернет

PC1> ping ya.ru

ya.ru resolved to 77.88.44.242

84 bytes from 77.88.44.242 icmp_seq=1 ttl=56 time=9.907 ms

84 bytes from 77.88.44.242 icmp_seq=2 ttl=56 time=10.354 ms

84 bytes from 77.88.44.242 icmp_seq=3 ttl=56 time=13.094 ms

84 bytes from 77.88.44.242 icmp_seq=4 ttl=56 time=16.578 ms

84 bytes from 77.88.44.242 icmp_seq=5 ttl=56 time=12.613 ms

PC2> ping cisco.com

cisco.com resolved to 72.163.4.185

84 bytes from 72.163.4.185 icmp_seq=1 ttl=46 time=163.881 ms

84 bytes from 72.163.4.185 icmp_seq=2 ttl=46 time=163.377 ms

84 bytes from 72.163.4.185 icmp_seq=3 ttl=46 time=164.746 ms

84 bytes from 72.163.4.185 icmp_seq=4 ttl=46 time=164.599 ms

84 bytes from 72.163.4.185 icmp_seq=5 ttl=46 time=163.202 ms

Проверяем таблицу преобразований адресов на vesr124-2-1

show ip nat translation

vesr124-2-1# sh ip nat translations

Prot	Inside source	Inside destination	Outside source
Outside destination	Pkts	Bytes	
----	-----	-----	-----
icmp	172.16.1.200	72.163.4.185	192.168.10.74
72.163.4.185	--	--	
icmp	172.16.1.200	72.163.4.185	192.168.10.74
72.163.4.185	--	--	
icmp	172.16.1.200	72.163.4.185	192.168.10.74
72.163.4.185	--	--	
icmp	172.16.1.100	77.88.55.242	192.168.10.74
77.88.55.242	--	--	
icmp	172.16.1.100	77.88.55.242	192.168.10.74
77.88.55.242	--	--	
icmp	172.16.1.100	77.88.55.242	192.168.10.74
77.88.55.242	--	--	
icmp	172.16.1.200	72.163.4.185	192.168.10.74
72.163.4.185	--	--	
icmp	172.16.1.200	72.163.4.185	192.168.10.74
72.163.4.185	--	--	
icmp	172.16.1.100	77.88.55.242	192.168.10.74
77.88.55.242	--	--	
icmp	172.16.1.100	77.88.55.242	192.168.10.74
77.88.55.242	--	--	
udp	172.16.1.200:14503	77.88.8.8:53	192.168.10.74:14503
77.88.8.8:53	--	--	
icmp	172.16.1.200	72.163.4.185	192.168.10.74
72.163.4.185	--	--	

udp	172.16.1.100:28458	77.88.8.8:53	192.168.10.74:28458
77.88.8.8:53	--	--	
icmp	172.16.1.200	72.163.4.185	192.168.10.74
72.163.4.185	--	--	
icmp	172.16.1.200	72.163.4.185	192.168.10.74
72.163.4.185	--	--	

В итоге такая конфигурация виртуального маршрутизатора достаточна для обеспечения минимально защищенного доступа в сеть Интернет сети домашнего офиса.

ВЫВОДЫ ПО ГЛАВЕ

- Принцип работы протокола SNAT
- Преимущества и недостатки SNAT
- Настройка сервера SNAT
- Проверка работы трансляции исходящих сетевых адресов

Как результат работы получена рабочая схема с SNAT (Source NAT) и клиенты локальной сети получили выход в интернет из локальной сети.

В следующей главе вы узнаете как настроить доступ по протоколу SSH к машине с Linux из локальной сети.

Глава 6. Настройка SSH в виртуальном маршрутизаторе vESR.

Цель работы:

Настроить доступ по протоколу SSH к машине с Linux в локальной сети.

Общее определение этого протокола из источников во всемирной паутине таково:

SSH (Secure Shell) — это протокол, который помогает безопасно подключаться к удалённому устройству и управлять им через командную строку. Он шифрует весь трафик, включая команды и пароли, защищает соединение от прослушивания и атак.

Вот для чего нужен SSH:

- **Удалённое управление серверами.** Главная задача SSH — позволить администраторам и разработчикам управлять удалёнными компьютерами, как будто они сидят за ними.
- **Поддержка пользователей.** Техническая поддержка может подключиться к компьютеру пользователя, чтобы помочь решить проблему: установить программу, настроить систему или удалить вирус. Например, новый сотрудник находится за границей и нужно настроить ему доступ к почте и аналитическим отчётам.
- **Работа из любой точки мира.** Благодаря SSH IT-специалисты могут работать дома, в дороге или в другой стране. Например, [DevOps-инженеру](#) в командировке пришло уведомление о сбое на сервере. Он может открыть ноутбук, подключиться по SSH и перезапустить нужную службу.
- **Автоматизация и мониторинг.** Удалённый доступ часто используют для запуска скриптов, мониторинга работы приложений или обновлений. При этом сотруднику не обязательно находиться на рабочем месте в офисе. Например, с помощью SSH запускают скрипт, который обновляет сайты каждую ночь на удалённом сервере.
- **Передача файлов между машинами.** С помощью утилит `scp` или `sftp` можно безопасно копировать файлы между устройствами по SSH.
- **Безопасная работа с Git и другими сервисами.** Многие сервисы вроде [GitHub](#), GitLab, Bitbucket поддерживают работу по SSH. Можно, например, работать с репозиториями без постоянного ввода пароля.
- **Доступ к внутренним службам.** С помощью SSH можно прокидывать

порты, то есть безопасно получать доступ к внутренним службам, которые не доступны из интернета. Например, когда нужно подключиться к базе данных на сервере, которая доступна только локально.

Системному администратору доступ к устройству по протоколу SSH предоставляет широкие возможности по контролю, конфигурации и поиску неисправностей. Поэтому рассмотрим настройку виртуального маршрутизатора в качестве сервера SSH.

В заводской конфигурации [vESR](#) разрешен удаленный доступ к маршрутизатору по протоколам Telnet или SSH из зоны «TRUSTED». Для того чтобы разрешить удаленный доступ к маршрутизатору из других зон, например, из публичной сети, необходимо создать соответствующие правила в firewall. Сначала рассмотрим доступ из локальной сети.

Для проверки доступа из локальной сети нужно добавить еще одно устройство, которое содержит клиент ssh. Добавление виртуальных устройств в GNS3 (appliance) написано на сайте <https://docs.gns3.com/docs/using-gns3/beginners/import-gns3-appliance> . Это может быть linux или Windows виртуальная машины, интегрированная в GNS3. Из бесплатных вариантов на сайте GNS3 я выбрал Micro Core Linux <https://www.gns3.com/gns3/appliance/download?url=https%3A%2F%2Fraw.githubusercontent.com%2FGNS3%2Fgns3-registry%2Fmaster%2Fappliances%2Fmicrocore-linux.gns3a>

Поскольку он самый не требовательный к ресурсам хостового ПК и в сети много материалов посвящённых ему, например официальный сайт

После добавления этого маленького образа Linux в GNS3 нужно будет еще обновить его пакетную базу и установить сервер и клиента ssh. По умолчанию в этом Линуксе Login gns3, password gns3:

```
gns3@box:/usr/local/etc/ssh$ tce-update
```

Checking for Easy Mode Operation... OK

Press Enter key to begin batch update of extensions in /sda1/tce

or enter any char to exit now:

Checking Tiny Core Applications in /mnt/sda1/tce/optional

Your system is up-to-date.

Press Enter key.

gns3@box:/usr/local/etc/ssh\$

gns3@box:~\$ tce-load -wi openssh

openssh.tcz.dep OK

Downloading: openssl.tcz

Connecting to repo.tinycorelinux.net (128.127.66.77:80)

openssl.tcz 100% |*****| 1116k

0:00:00 ETA

openssl.tcz: OK

Downloading: openssh.tcz

Connecting to repo.tinycorelinux.net (128.127.66.77:80)

openssh.tcz 100% |*****| 1992k

0:00:00 ETA

openssh.tcz: OK

gns3@box:~\$ cd /usr/local/etc/init.d/ ssh/

gns3@box:/usr/local/etc/ssh\$ sudo /usr/local/etc/init.d/openssh start

gns3@box:/usr/local/etc/ssh\$

Проверка работы сервиса SSH:

```
gns3@box:~$ netstat -an | grep 22

tcp      0      0 0.0.0.0:22          0.0.0.0:*          LISTEN
tcp      0      0 :::22              :::*                LISTEN
```

Для того, чтобы сервис SSH автоматически запускался при старте виртуальной машины нужно внести изменения в два конфигурационных файла:

```
gns3@box:~$ sudo vi /opt/.filetool.lst

opt
home
etc/issue
etc/shadow
etc/inittab
etc/securetty
```

```
/opt/bootlocal.sh
/usr/local/etc/init.d/openssh
```

Добавьте в конец файла /opt/.filetool.lst две строки, выделенный красным прямоугольником.

Изменения нужно сохранить:

```
gns3@box:~$ sudo vi /opt/.filetool.lst

gns3@box:~$ filetool.sh -b

Backing up files to /mnt/sda1//mydata.tgz
```

Измените файл /opt/bootlocal.sh:

```
gns3@box:~$ sudo vi /opt/bootlocal.sh

#!/bin/sh

# put other system startup commands here
```

```
/usr/local/etc/init.d/openssh start
```

```
~
```

Изменения нужно сохранить:

```
gns3@box:~$ sudo vi /opt/.filetool.lst

gns3@box:~$ filetool.sh -b

Backing up files to /mnt/sda1//mydata.tgz
```

Схема теперь выглядит так:

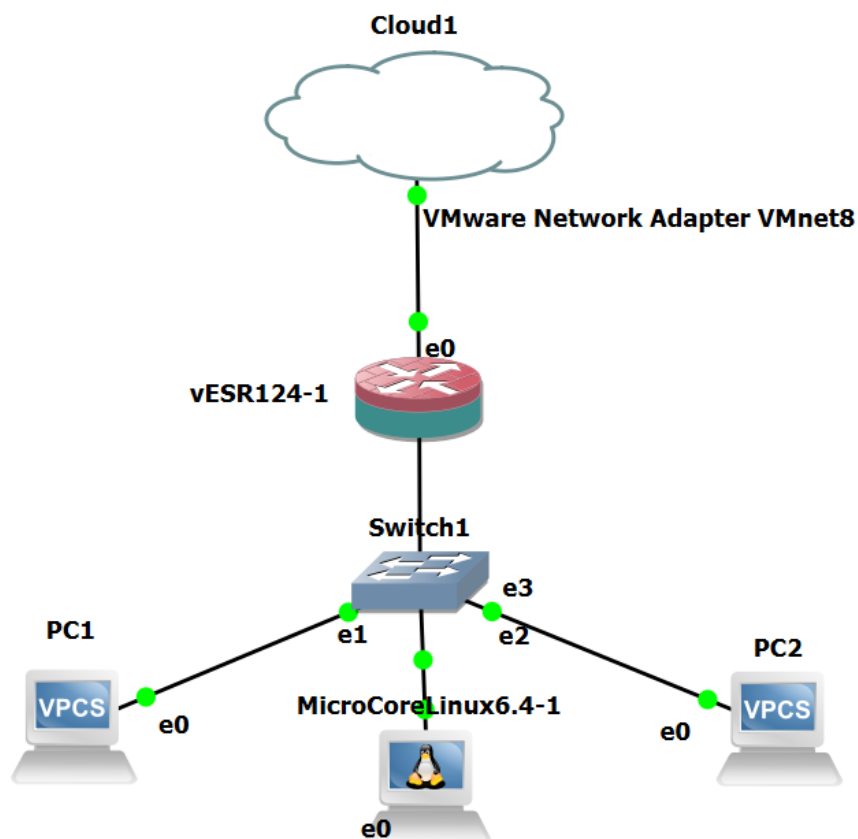


РИСУНОК 6-1. КОПИЯ ЭКРАНА СО СХЕМОЙ СТЕНДА.

В начале проверим, что доступа по 22 порту (SSH) у нас с линуксовой машины на виртуальный маршрутизатор нету:

```

root@box:/home/gns3# netstat -an | grep 22

tcp    0    0 0.0.0.0:22          0.0.0.0:*          LISTEN
tcp    0    0 :::22             :::*               LISTEN

root@box:/home/gns3# telnet 172.16.1.2 22

telnet: can't connect to remote host (172.16.1.2): No route to host

```

При конфигурировании доступа к маршрутизатору правила создаются для пары зон:

- **source-zone** – зона, из которой будет осуществляться удаленный доступ, в нашем случае это зона **TRUSTED**;
- **self** – зона, в которой находится интерфейс управления маршрутизатором.

Для создания разрешающего правила используются следующие команды:

- общий синтаксис:

```
vesr124-2-1# configure
vesr124-2-1(config)# security zone-pair TRUSTED self
vesr124-2-1(config-zone-pair)# rule <number>
vesr124-2-1(config-zone-rule)# action permit
vesr124-2-1(config-zone-rule)# match protocol tcp
vesr124-2-1(config-zone-rule)# match source-address <network object-
group>
vesr124-2-1(config-zone-rule)# match destination-address <network
object-group>
vesr124-2-1(config-zone-rule)# match source-port any
vesr124-2-1(config-zone-rule)# match destination-port <service object-
group>
vesr124-2-1(config-zone-rule)# enable
vesr124-2-1(config-zone-rule)# exit
vesr124-2-1(config-zone-pair)# exit
```

Пример команд для разрешения пользователям из зоны **TRUSTED** с IP-адресами локальной сети 172.16.1.1/24 подключаться к маршрутизатору с IP-адресом 172.16.1.1 по протоколу SSH:

```
configure

object-group LAN_GATEWAY

ip address-range 209.100.1.1--172.16.1.254 # IP-адреса локальной
сети

exit

object-group LAN

ip address-range 172.16.1.1 # IP-адрес виртуального маршрутизатора
vesr124-2-1- смотрящий в сторону PC1, PC2 и MicroCore Linux

exit

Copy

do commit

do confirm

Copy

object-group service ssh

port-range 22

exit

Copy

do commit

do confirm
```

```
vesr124-2-1# config

vesr124-2-1(config)# object-group service ssh

vesr124-2-1(config-object-group-service)# port-range 22

vesr124-2-1(config-object-group-service)# exit
```

```
vesr124-2-1(config)# do commit
```

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

2025-05-30T14:03:40+00:00 %CLI-I-CRIT: user admin from console
input: do commit

```
vesr124-2-1(config)# do confirm
```

Configuration has been confirmed. Commit timer canceled.

2025-05-30T14:03:46+00:00 %CLI-I-CRIT: user admin from console
input: do confirm

```
vesr124-2-1(config)#
```

```
security zone-pair TRUSTED self
```

```
rule 3
```

```
action permit
```

```
match protocol tcp
```

```
match source-address COMPANY
```

```
match destination-address COMPANY_GATEWAY
```

```
match source-port any
```

```
match destination-port ssh
```

```
enable
```

```
exit
```

```
exit
```

```
do commit
```

do confirm

```
vesr124-2-1(config)# security zone-pair TRUSTED self
vesr124-2-1(config-security-zone-pair)# rule 3
vesr124-2-1(config-security-zone-pair-rule)# action permit
vesr124-2-1(config-security-zone-pair-rule)# match protocol tcp
vesr124-2-1(config-security-zone-pair-rule)# match source-address
object-group LAN_GATEWAY
vesr124-2-1(config-security-zone-pair-rule)# match destination-address
object-group LAN
vesr124-2-1(config-security-zone-pair-rule)# match source-port any
vesr124-2-1(config-security-zone-pair-rule)# match destination-port any
Check match any TCP/UDP port
object-group Check match by object group
port-range Check match by port range
vesr124-2-1(config-security-zone-pair-rule)# match destination-port
object-group ssh
vesr124-2-1(config-security-zone-pair-rule)# enable
vesr124-2-1(config-security-zone-pair-rule)# exit
vesr124-2-1(config-security-zone-pair)# exit
vesr124-2-1(config)# do commit

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

```
2025-05-30T14:18:41+00:00 %CLI-I-CRIT: user admin from console
input: do commit

vesr124-2-1(config)# do confirm

Configuration has been confirmed. Commit timer canceled.

2025-05-30T14:18:46+00:00 %CLI-I-CRIT: user admin from console
input: do confirm

vesr124-2-1(config)# do save

Configuration has been successfully saved

vesr124-2-1(config)#
```

Проверяем доступ по SSH с MINI Core Linux:

```
gns3@box:~$ ssh admin@172.16.1.1

The authenticity of host '172.16.1.1 (172.16.1.1)' can't be established.

ECDSA key fingerprint is
a3:bc:d0:72:71:e3:f7:50:58:43:39:77:c3:2c:f5:95.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added '172.16.1.1' (ECDSA) to the list of known
hosts.

admin@172.16.1.1's password:

*****

*           Welcome to vESR           *

*****

vesr124-2-1#
```

Из локальной сети за маршрутизатором доступ по протоколу SSH есть.

При конфигурировании доступа к маршрутизатору правила создаются для пары зон:

- **source-zone** – зона, из которой будет осуществляться удаленный доступ, в нашем случае это зона **TRUSTED**;
- **self** – зона, в которой находится интерфейс управления маршрутизатором.

К группе сетевых объектов WAN нужно ещё добавить группу клиентов SSH:

```
vesr124-2-1# config
vesr124-2-1(config)#object-group network clients
vesr124-2-1(config-object-group-network)# ip address-range
192.168.10.0-192.168.10.254
vesr124-2-1(config-object-group-network)# exit
vesr124-2-1( config)#
```

Вводим команды для разрешения пользователю из зоны «**UNTRUSTED**» с IP-адресами из сети 192.168.10.1/24 подключаться к маршрутизатору с IP-адресом 192.168.10.50 (адрес внешнего интерфейса gi1/0/1 виртуального маршрутизатора vesr124-2-1, полученный командой sh ip int) по протоколу SSH:

```
vesr124-2-1(config)# security zone-pair UNTRUSTED self
vesr124-2-1(config-security-zone-pair)# rule 10
vesr124-2-1(config-security-zone-pair-rule)# action permit
vesr124-2-1(config-security-zone-pair-rule)# match protocol tcp
```

```
vesr124-2-1(config-security-zone-pair-rule)#  
vesr124-2-1(config-security-zone-pair-rule)# match source-address object-group clients  
vesr124-2-1(config-security-zone-pair-rule)# match destination-address object-group WAN  
vesr124-2-1(config-security-zone-pair-rule)# match destination-port object-group ssh  
vesr124-2-1(config-security-zone-pair-rule)#  
vesr124-2-1(config-security-zone-pair-rule)# enable  
vesr124-2-1(config-security-zone-pair-rule)# exit  
vesr124-2-1(config-security-zone-pair)# exit  
vesr124-2-1(config)#do commit  
vesr124-2-1(config)#do confirm  
vesr124-2-1(config)#exit
```

В OS виртуальных маршрутизаторов vesr нет команд мониторинга работы пользователей сессий SSH. Есть только возможность просмотра лога событий:

```
vesr124-2-1# sh syslog tmpsys:syslog/auth.log | i ssh
```

```
2025-06-05T10:47:01+00:00 %AAA-I-SSH: Accepted password for  
admin from 192.168.10.112 port 42242 ssh2
```

```
2025-06-05T10:47:01+00:00 %AAA-LOCAL-I-SESSION: ssh: session  
opened for user admin
```

```
vesr124-2-1#
```

Видно, что подключился внешний пользователь с адресом 192.168.10.112 и открыл сессию SSH с логином admin.

Адрес 192.168.10.112 выдан моему планшету домашним роутером по DHCP протоколу.

На Рис. Фито экрана планшета с запущенным сеансом ssh в приложении ConnectBot.

Лабораторные работы с виртуальным сервисным маршрутизатором vESR
В графическом симуляторе GNS3

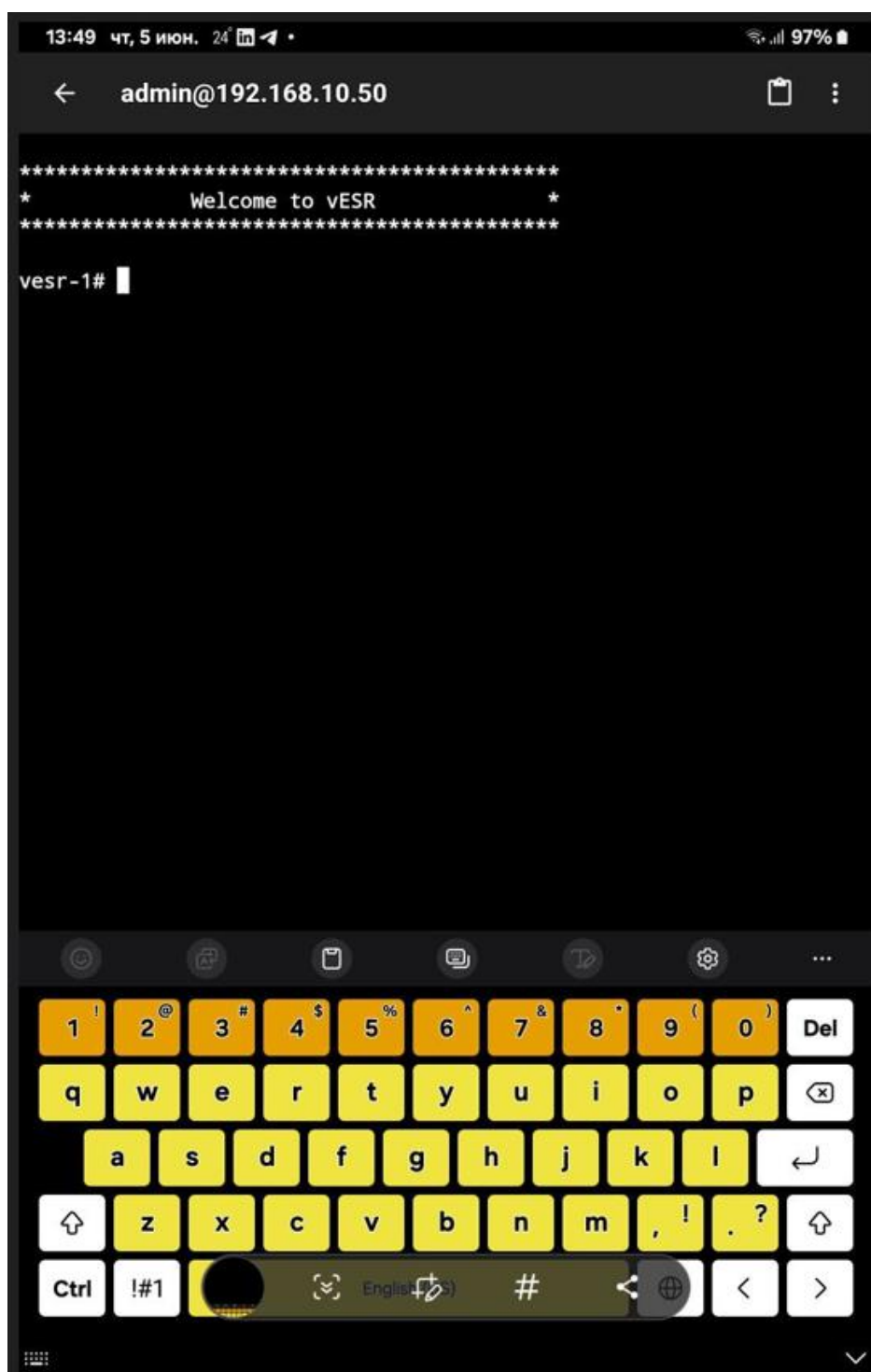


РИСУНОК 6-2. ИЗОБРАЖЕНИЕ С ЭКРАНА ПЛАНШЕТА С ТЕРМИНАЛОМ СВЯЗИ.

Точно так же проверяется доступ с любого сетевого адреса из сети 192.168.10.0/24 (за исключением адреса собственной хостовой машины) – например у меня запущена виртуальная машина с Ubuntu:

```
rinat@ubuntu22:~$ ip add | grep 'ens' || 'inet'

2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500
qdisc fq_codel state UP group default qlen 1000

    inet 192.168.10.31/24 brd 192.168.10.255 scope global ens33

3: ens37: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state
DOWN group default qlen 1000

rinat@ubuntu22:~$ ssh rinat@192.168.10.50

rinat@192.168.10.50's password:

*****

*           Welcome to vESR           *

*****

vesr124-2-1# sh syslog tmpsys:syslog/auth.log | i ssh
```

```
2025-06-05T11:54:30+00:00 %AAA-I-SSH: Accepted password for rinat
from 192.168.10.31 port 47820 ssh2
```

```
2025-06-05T11:54:30+00:00 %AAA-LOCAL-I-SESSION: ssh: session
opened for user rinat
```

ВЫВОДЫ ПО ГЛАВЕ

- что такое SSH
- назначение SSH
- настройка сервера SSH на машине с Linux
- настройка зон безопасности для портов ssh на маршрутизаторе для доступа к серверу SSH
- проверка работы

В следующей главе вы узнаете что такое Destination NAT (DNAT) и как его настроить на маршрутизаторе.

Глава 7. Настройка NAT(DNAT) для доступа в Интернет в виртуальном маршрутизаторе vESR.

Цель работы:

Ознакомится с работой протокола и научиться настраивать DNAT в маршрутизаторе.

- Общее определение что такое протокол DNAT из доступных источников в интернет следующее-DNAT (Destination Network Address Translation) — это тип технологии NAT (Network Address Translation), которая изменяет адрес и порт назначения входящего пакета. newstorial.comexpertnetworkconsultant.comdocs.selectel.ru

Механизм работы DNAT включает три этапа: newstorial.com

Анализ входящего пакета. Устройство (маршрутизатор или фаервол) проверяет адрес назначения и номер порта. newstorial.com

Преобразование. На основе заранее определённых правил маршрутизатор или фаервол заменяет адрес назначения и, возможно, номер порта. newstorial.com

Направление пакета. После преобразования пакет отправляется к новому адресу внутри частной сети. newstorial.com

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

Перенаправление портов. Позволяет внешним устройствам получать доступ к сервисам в частной сети, сопоставляя внешний порт с внутренним IP-адресом и портом. newstorial.comdocs.ideco.dev

Настройка виртуальных частных сетей (VPN). DNAT перенаправляет трафик из публичной сети в частную, что помогает обеспечить безопасность соединения. newstorial.com

С помощью DNAT трафик, приходящий на определённый порт одного сервера (обычно шлюза), автоматически пересылается на другой IP и/или порт внутри сети. arenda-server.cloud

○ Некоторые цели использования DNAT:

-
- доступ к внутренним сервисам из интернета (веб, SSH, RDP, FTP и т.д.);
- проброс портов для VPN, игровых серверов, VoIP;

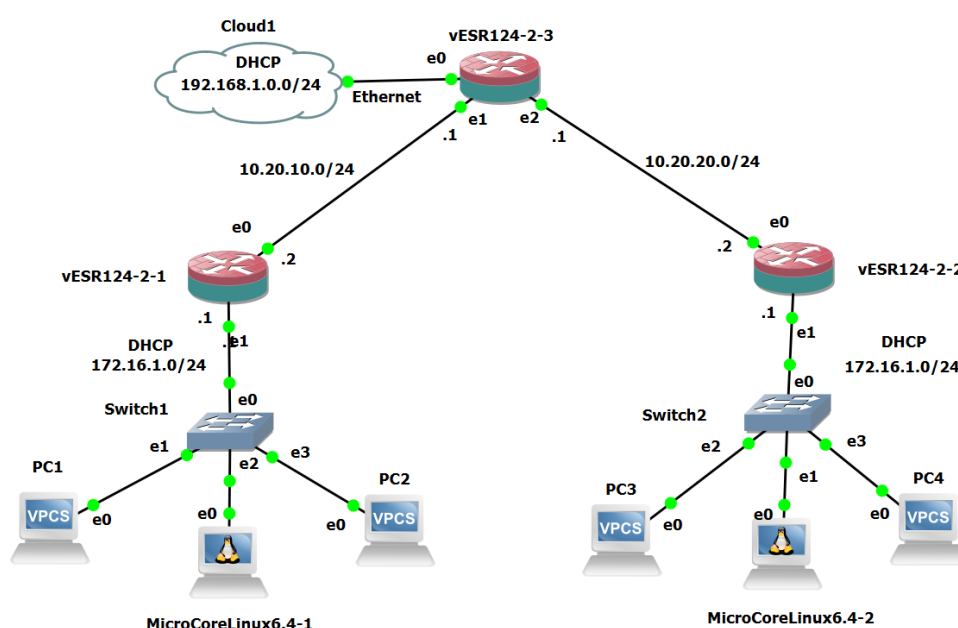
- организация DMZ (демилитаризованной зоны) для публичных сервисов;
 - экономия на публичных IP: один внешний адрес — много внутренних сервисов;
 - тестирование и разработка: проброс портов для контейнеров, виртуалок, CI/CD.
- Настройка и конфигурация DNAT маршрутизатора.

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 vesr124-2-1), 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 в 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 vesr124-2-1.



**РИСУНОК 7-1 СХЕМА СВЯЗИ ДОМАШНЕГО ОФИСА С ФИЛИАЛАМ ЧРЕЗ
ПРОВАЙДЕРА ИНТЕРНЕТ.**

Настройка центрального виртуального маршрутизатора **vesr124-2-3**:
Дадим ему название, выключим межсетевой экран и назначим IP
адрес на интерфейсе **gi1/0/1**:

```
vesr(config)# hostname vesr124-2-3
vesr(config)# exit
vesr(config)# do commit
vesr(config)# do confirm
vesr124-2-3(config)# int gigabitethernet 1/0/1
vesr124-2-3(config-if-gi)# description "link2 vesr124-2-1"
vesr124-2-3(config-if-gi)# ip firewall disable
vesr124-2-3(config-if-gi)# ip address 10.10.10.1/24
vesr124-2-3(config-if-gi)# exit
vesr(config)# do commit
vesr(config)# do confirm
```

так же настроим второй интерфейс:

```
vesr124-2-3(config)# int gigabitethernet 1/0/2
vesr124-2-3(config-if-gi)# description "link2 vesr124-2-2"
vesr124-2-3(config-if-gi)# ip firewall disable
vesr124-2-3(config-if-gi)# ip address 10.10.20.1/24
vesr124-2-3(config-if-gi)# exit
vesr124-2-3(config)# do commit
```

```

vesr124-2-3(config)# do confirm
Включим маршрутизацию на обе ветки с подключенными сетями:
vesr124-2-3(config)# ip route 10.10.10.0/24 interface gigabitethernet
1/0/2
vesr124-2-3(config)# ip route 10.10.20.0/24 interface gigabitethernet
1/0/3
vesr124-2-3(config)# do commit
vesr124-2-3(config)# do confirm
vesr124-2-3(config)# exit

```

От центрального маршрутизатора понадобится только простая маршрутизация пакетов IP. Он здесь выступает в роли интернет сервис-провайдера. Поэтому межсетевой экран на обоих интерфейсах отключен.

Добавляем маршрутизацию по умолчанию и маршруты к сетям клиентов в левой и правой частях схемы, которые находятся за виртуальными маршрутизаторами vesr124-2-1 vesr124-2-2 соответственно:

```

vesr124-2-3#config
vesr124-2-3(config)#
vesr124-2-3(config)# ip route 0.0.0.0/0 192.168.10.1
vesr124-2-3(config)# ip route 172.16.1.0/24 10.10.10.2
vesr124-2-3(config)# ip route 172.16.2.0/24 10.10.20.2
Добавляем вывод диагностических сообщений в консоль при
загрузке:
vesr124-2-3(config)#
vesr124-2-3(config)#syslog console
vesr124-2-3(config-syslog console)# virtual-serial
vesr124-2-3(config)#exit

```

Настраиваем NAT с заменой адресов источника на адрес выходного интерфейса (SNAT) для работы клиентов в Интернет:

```

vesr124-2-3# config
vesr124-2-3(config)# nat source
vesr124-2-3(config-snat)# pool UPLINK
vesr124-2-3(config-snat-pool)# ip address-range 192.168.10.114
vesr124-2-3(config-snat-pool)# exit
vesr124-2-3(config-snat)# ruleset SNAT
vesr124-2-3(config-snat-ruleset)# to interface gigabitethernet 1/0/1
vesr124-2-3(config-snat-ruleset)# rule 8

```

```

vesr124-2-3(config-snat-rule)# match source-address address-
range 10.10.20.2
-10.10.20.254
vesr124-2-3(config-snat-rule)# action source-nat pool UPLINK
vesr124-2-3(config-snat-rule)# enable
vesr124-2-3(config-snat-rule)# exit

vesr124-2-3(config-snat-ruleset)# rule 9

vesr124-2-3(config-snat-rule)# match source-address address-
range 10.10.10.2
-10.10.10.254
vesr124-2-3(config-snat-rule)# action source-nat pool UPLINK
vesr124-2-3(config-snat-rule)# enable
vesr124-2-3(config-snat-rule)# exit
vesr124-2-3(config-snat-ruleset)# rule 10
vesr124-2-3(config-snat-rule)# match source-address address-range
10.10.30.1
-10.10.30.254
vesr124-2-3(config-snat-rule)# action source-nat pool UPLINK
vesr124-2-3(config-snat-rule)# enable
vesr124-2-3(config-snat-rule)# exit
vesr124-2-3(config-snat-ruleset)# exit
vesr124-2-3(config-snat)# exit
vesr124-2-3(config)#

```

Здесь адрес 192.168.10.114 выдан по DHCP провайдером Интернет интерфейсу виртуального маршрутизатора vesr124-2-3. Именно он и будет заменяться на исходящие адреса от клиентов сетей 10.10.10.0/24 и 10.10.20.0/24 и 10.10.30.0/24 (понадобится в дальнейших лабораторных работах) в пакетах IP.

```

vesr124-2-3(config)# do commit
vesr124-2-3(config)# do confirm
vesr124-2-3(config)# exit

```

На этом настройка центрального виртуального маршрутизатора завершена.

Настройка виртуального маршрутизатора vesr124-2-1(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.

```
vesr124-2-1# configure
vesr124-2-1(config)# security zone UNTRUST
vesr124-2-1(config-zone)# exit
vesr124-2-1(config)# security zone TRUST
vesr124-2-1(config-zone)# exit
vesr124-2-1(config)# interface gigabitethernet 1/0/1
vesr124-2-1(config-if-gi)# security-zone UNTRUST
vesr124-2-1(config-if-gi)# ip address 10.10.10.1/24
vesr124-2-1(config-if-gi)# exit
vesr124-2-1(config)# interface gigabitethernet 1/0/2
vesr124-2-1(config-if-te)# ip address 172.16.1.1/24
vesr124-2-1(config-if-te)# security-zone TRUST
vesr124-2-1(config-if-te)# exit
```

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

WAN – профиль адресов публичной сети (выход в Интернет);

LAN_NETWORK – профиль адресов локальной сети (сеть локальная);

SSH – профиль портов (какой порт будет заменяться при доступе извне).

SERVER_IP – профиль адреса сервера ssh.

```
vesr124-2-1(config)# object-group network WAN
vesr124-2-1(config-object-group-network)# ip address 10.10.10.2
vesr124-2-1(config-object-group-network)# exit
vesr124-2-1(config)# object-group service SSH
vesr124-2-1(config-object-group-network)# port-range 2222
vesr124-2-1(config-object-group-network)# exit
vesr124-2-1(config)# object-group network SERVER_IP
vesr124-2-1(config-object-group-network)# ip address-range 172.16.1.1
vesr124-2-1(config-object-group-network)# ip address 172.16.1.3
vesr124-2-1(config-object-group-network)# exit
vesr124-2-1(config)# object-group network LAN_GW
vesr124-2-1(config-object-group-network)# ip address-range
172.16.1.1-172.16.1.254
vesr124-2-1(config-object-group-network)# exit
vesr124-2-1(config)# exit
```

Зафиксируем выдаваемый по DHCP адрес клиенту MicroCoreLinux6.4-1 в настройках сервера DHCP на виртуальном маршрутизаторе vesr124-2-1, предварительно узнав в консоли клиента Линукс MAC адрес его сетевого интерфейса eth0:

```
box login: gns3
Password:gns3
( '>')
/) TC (\ Core is distributed with ABSOLUTELY NO WARRANTY.
(/-__-_)      www.tinycorelinux.net
gns3@box:~$ ip link | grep -C 1 eth0 | grep link/ether
link/ether 0c:28:d9:73:00:00 brd ff:ff:ff:ff:ff:ff
gns3@box:~$
```

MAC адрес получен. Фиксируем его в выдаче:

```
vesr124-2-1# config
vesr124-2-1(config)# ip dhcp-server
vesr124-2-1(config)# ip dhcp-server pool LAN_NETWORK
vesr124-2-1(config-dhcp-server)# network 172.16.1.0/24
vesr124-2-1(config-dhcp-server)# default-lease-time 003:00:00
vesr124-2-1(config-dhcp-server)# address-range 172.16.1.1-
172.16.1.254
vesr124-2-1(config-dhcp-server)# address 172.16.1.2 mac-address
0c:28:d9:73:00:00
vesr124-2-1(config-dhcp-server)# default-router 172.16.1.1
vesr124-2-1(config-dhcp-server)# dns-server 77.88.8.8
vesr124-2-1(config-dhcp-server)# exit
vesr124-2-1(config)#
```

Для обновлений пакетов в клиенте с линуксом и для проверки нужно сделать SNAT :

```
vesr124-2-1(config)# nat source
vesr124-2-1(config-snat)# pool WAN
vesr124-2-1(config-snat-pool)# ip address-range 10.10.10.2
vesr124-2-1(config-snat-pool)# exit
vesr124-2-1(config-snat)# ruleset SNAT
vesr124-2-1(config-snat-ruleset)# to zone UNTRUST
vesr124-2-1(config-snat-ruleset)# rule 1
```

```

vesr124-2-1(config-snat-rule)# match source-address object-group
LAN_NETWORK
vesr124-2-1(config-snat-rule)# action source-nat interface
vesr124-2-1(config-snat-rule)# enable
vesr124-2-1(config-snat-rule)# exit
vesr124-2-1(config-snat-ruleset)# exit
vesr124-2-1(config-snat)# exit
vesr124-2-1(config)#

```

Прописываем всю необходимую маршрутизацию согласно приведенной выше схеме на Рис.:

```

vesr124-2-1(config)# ip route 0.0.0.0/0 10.10.10.1
vesr124-2-1(config)# ip route 10.10.20.0/24 10.10.20.1
vesr124-2-1(config)# ip route 10.10.30.0/24 10.10.30.1
vesr124-2-1(config)# ip route 172.16.2.0/24 10.10.20.2
vesr124-2-1(config)# ip route 172.16.1.0/24 interface gigabitethernet
1/0/2
vesr124-2-1(config)#

```

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.

```

vesr124-2-1(config)# nat destination
vesr124-2-1(config-dnat)# pool SERVER_POOL
vesr124-2-1(config-dnat-pool)# ip address 172.16.1.2
vesr124-2-1(config-dnat-pool)# ip port 22
vesr124-2-1(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 порту назначения (match destination-address, match destination-port). Кроме этого в наборе задано действие, применяемое к данным, удовлетворяющим всем правилам (action destination-nat). Набор правил вводится в действие командой «enable».

```

vesr124-2-1(config-dnat)# ruleset DNAT
vesr124-2-1(config-dnat-ruleset)# from zone UNTRUST
vesr124-2-1(config-dnat-ruleset)# rule 1

```

```

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.

```

vesr124-2-1(config)#
vesr124-2-1(config)# security zone-pair UNTRUST TRUST
vesr124-2-1(config-security-zone-pair)# rule 1
vesr124-2-1(config-security-zone-pair-rule)# action permit
vesr124-2-1(config-security-zone-pair-rule)# match protocol icmp
vesr124-2-1(config-security-zone-pair-rule)# enable
vesr124-2-1(config-security-zone-pair-rule)# exit
vesr124-2-1(config-security-zone-pair)# rule 10
vesr124-2-1(config-security-zone-pair-rule)# action permit
vesr124-2-1(config-security-zone-pair-rule)# match protocol tcp
vesr124-2-1(config-security-zone-pair-rule)# match destination-
address object-group SERVER_IP
vesr124-2-1(config-security-zone-pair-rule)# enable
vesr124-2-1(config-security-zone-pair-rule)# exit
vesr124-2-1(config-security-zone-pair)# exit
vesr124-2-1(config)#

```

Изменения конфигурации вступят в действие после применения:

```

vesr124-2-1# commit
Configuration has been successfully committed
esr# confirm

```

Configuration has been successfully confirmed

Произведенные настройки можно посмотреть с помощью команд:

```

vesr124-2-1# show ip nat destination pools
vesr124-2-1# show ip nat destination rulesets
vesr124-2-1# show ip nat proxy-arp
vesr124-2-1# show ip nat translations

```

Проверяем 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:

```
vesr124-2-3# 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
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:
vesr124-2-1# sh ip nat translations

```

Prot	Inside source	Inside destination	Outside source
icmp	172.16.1.3	10.10.20.1	10.10.10.2

```

10.10.20.1      --      --
vesr124-2-1# sh ip nat translations

```

Prot	Inside source	Inside destination	Outside source
tcp	10.10.10.1:38358	172.16.1.3:22	10.10.10.1:38358
icmp	172.16.1.3	10.10.20.1	10.10.10.2
icmp	172.16.1.3	1.1.1.1	10.10.10.2
udp	172.16.1.3:43522	77.88.8.8:53	10.10.10.2:43522

```

77.88.8.8:53      --      --
vesr124-2-1# sh ip nat destination pools

```

Name	IP	Port	Description
------	----	------	-------------

```

-----
SERVER_POOL          172.16.1.3    22    --
vesr124-2-1# sh ip nat destination rulesets
Name                  From          Description
-----
DNAT                  zone 'UNTRUST'  --
vesr124-2-1#

```

DNAT на виртуальном маршрутизаторе vesr124-2-1и маршрутизация на vesr124-2-3 работают.

Для закрепления полученного навыка повторим шаги описанные в предыдущих главах применив их к новому малому офису.

Переходим к настройке удаленного офиса с виртуальным маршрутизатором vesr124-2-2. Схема подключения аналогичная той, что была описана выше применительно к сети домашнего офиса. Подключена эта сеть к интерфейсу gi1/0/2 виртуального маршрутизатора vesr124-2-3 с IP адресом 10.10.20.1. Следовательно, назначим IP адрес 10.10.20.2 интерфейсу Gi1/0/1 виртуального маршрутизатора vesr124-2-2 не забыв создать зоны контроля:

```

vesr124-2-2#config
vesr124-2-2(config)# security zone UNTRUST
vesr124-2-2(config-security-zone)#exit
vesr124-2-2(config)# security zone TRUST
vesr124-2-2(config-security-zone)#exit
vesr124-2-2(config)# security zone TRUST
vesr124-2-2(config-security-zone)# exit
vesr124-2-2(config)# int gigabitethernet 1/0/1
vesr124-2-2(config-if-gi)# description UPLINK
vesr124-2-2(config-if-gi)# ip address 10.10.20.2/24
vesr124-2-2(config-if-gi)# security-zone UNTRUST
vesr124-2-2(config-if-gi)# exit
vesr124-2-2(config)# int gigabitethernet 1/0/2
vesr124-2-2(config-if-gi)# description LAN2
vesr124-2-2(config-if-gi)# ip address 172.16.2.1/24
vesr124-2-2(config-if-gi)# security-zone TRUST
vesr124-2-2(config-if-gi)# exit
vesr124-2-2#config

```

Сохраняем конфиг и проверяем результат:

```
vesr124-2-2(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

vesr124-2-2(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

vesr124-2-2(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

vesr124-2-2(config)# do sh ip int

Type	IP address Precedence	Interface	Admin	Link
static	10.10.20.2/24 primary	gi1/0/1	Up	Up
static	172.16.2.1/24 primary	gi1/0/2	Up	Up

vesr124-2-2(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 vesr124-2-2 сервер DHCP для получения ими IP адресов автоматически:

```
vesr124-2-2(config)# ip dhcp-server pool LAN2
vesr124-2-2(config-dhcp-server)# network 172.16.2.0/24
vesr124-2-2(config-dhcp-server)# default-lease-time 3:00:00
vesr124-2-2(config-dhcp-server)# address-range 172.16.2.1-
172.16.2.254
vesr124-2-2(config-dhcp-server)# excluded-address-range 172.16.2.1
vesr124-2-2(config-dhcp-server)# excluded-address-range 172.16.2.254
vesr124-2-2(config-dhcp-server)# default-router 172.16.2.1
vesr124-2-2(config-dhcp-server)# dns-server 77.88.8.8
vesr124-2-2(config-dhcp-server)# exit
vesr124-2-2(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

vesr124-2-2(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

vesr124-2-2(config)#

В приведенном списке команда создается пул сервера DHCP с названием LAN2, резервируется сеть 172.16.2.0/24 класса C, 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 :

vesr124-2-2(config)# object-group service dhcp_service

vesr124-2-2(config-object-group-service)# port-range 68

vesr124-2-2(config-object-group-service)# exit

vesr124-2-2(config)# object-group service dhcp_client

vesr124-2-2(config-object-group-service)# port-range 68

vesr124-2-2(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:

vesr124-2-2(config)# object-group network GATEWAY_TO_LAN

vesr124-2-2(config-object-group-network)# ip address-range
172.16.2.1

vesr124-2-2(config-object-group-network)# exit

vesr124-2-2(config)# object-group network LAN_NETWORK

vesr124-2-2(config-object-group-network)# ip address-range
172.16.2.1-172.16.2.254

vesr124-2-2(config-object-group-network)# exit

vesr124-2-2(config)# object-group network WAN

vesr124-2-2(config-object-group-network)# ip address-range 10.10.20.1

vesr124-2-2(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:

```
vesr124-2-2(config)# security zone-pair TRUST self
vesr124-2-2(config-security-zone-pair)# rule 9
vesr124-2-2(config-security-zone-pair-rule)# match protocol icmp
vesr124-2-2(config-security-zone-pair-rule)# match destination-address
object-group LAN_NETWORK
vesr124-2-2(config-security-zone-pair-rule)# enable
vesr124-2-2(config-security-zone-pair-rule)# exit
vesr124-2-2(config-security-zone-pair)# exit
vesr124-2-2(config)# ip dhcp-server
vesr124-2-2(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

```
vesr124-2-2(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
vesr124-2-2(config)# exit
vesr124-2-2#

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 настройке 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:

```
vesr124-2-2#config
vesr124-2-2(config)#
: vesr124-2-2(config)# security zone-pair TRUST UNTRUST
vesr124-2-2(config-security-zone-pair)# rule 10
vesr124-2-2(config-security-zone-pair-rule)# match source-address
object-group LAN_NETWORK
vesr124-2-2(config-security-zone-pair-rule)# action permit
vesr124-2-2(config-security-zone-pair-rule)# enable
vesr124-2-2(config-security-zone-pair-rule)# exit
vesr124-2-2(config-security-zone-pair)# exit
vesr124-2-2(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
```

```
vesr124-2-2(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
vesr124-2-2(config)#
```

Конфигурируем сервис SNAT. Первым шагом задаётся IP-адрес публичной сети (WAN), используемых для сервиса SNAT:

```
vesr124-2-2(config)# nat source
vesr124-2-2(config-snat)# pool WAN
vesr124-2-2(config-snat-pool)# ip address-range 10.10.20.2
vesr124-2-2(config-snat-pool)# exit
vesr124-2-2(config-snat)#
```

Создаём набор правил SNAT. В атрибутах набора укажем, что правила применяются только для пакетов, направляющихся в публичную сеть – в зону UNTRUSTED. Правила включают проверку адреса источника данных на принадлежность к сети LAN_NETWORK:

```
vesr124-2-2(config-snat)# ruleset SNAT
vesr124-2-2(config-snat-ruleset)# to zone UNTRUST
vesr124-2-2(config-snat-ruleset)# rule 1
vesr124-2-2(config-snat-rule)# match source-address object-group
LAN_NETWORK
vesr124-2-2(config-snat-rule)# action source-nat pool WAN
vesr124-2-2(config-snat-rule)# enable
vesr124-2-2(config-snat-rule)# exit
vesr124-2-2(config-snat-ruleset)# exit
vesr124-2-2(config-snat)# exit
vesr124-2-2(config)# exit
```

Warning: you have uncommitted configuration changes.

```
vesr124-2-2# commit
```

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

```
2025-06-11T14:39:56+00:00 %CLI-I-CRIT: user admin from console
input: commit
vesr124-2-2# confirm
```

Configuration has been confirmed. Commit timer canceled.

```
2025-06-11T14:40:00+00:00 %CLI-I-CRIT: user admin from console
input: confirm
vesr124-2-2#
```

Источник документации к командам к виртуальному маршрутизатору: <https://docs.eltex-co.ru>

ВЫВОДЫ ПО ГЛАВЕ

- Что такое DNAT
- Назначение и возможные способы применения DNAT
- Создание нового узла сети-филиала
- Настройка конфигурации маршрутизатора в филиале
- Настройка DNAT на маршрутизаторе центрального офиса
- Проверка доступности центрального офиса из филиала.

В следующей главе вы узнаете как настроить защищенный туннель для связи локальных сетей филиала и центрального офиса.

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

Цель работы:

Создать L3VPN с помощью технологии GRE over IPSEC.

Что такое L3VPN (Layer 3 Virtual Private Network) — это технология виртуальной частной сети, которая работает на сетевом уровне модели OSI. Она использует IP-маршрутизацию и обеспечивает безопасную и эффективную передачу данных между серверами, расположенными в различных локациях через общедоступные или частные сети. GRE и IPsec применяются для создания защищённого и конфиденциального канала связи между сетями или устройствами. Это обеспечивает защиту данных при их передаче через потенциально недоверенные сети. создать условия защищенного соединения между удаленными офисами, центральным домашним и филиальным через Интернет с использованием топологии на схеме сети показанной на [Рис 8.1](#). Подготовить виртуальный маршрутизатор vesr для работы в симуляторе GNS3 с для организации защищённого соединения тоннелем с использованием комбинации протоколов GRE и IPSEC.

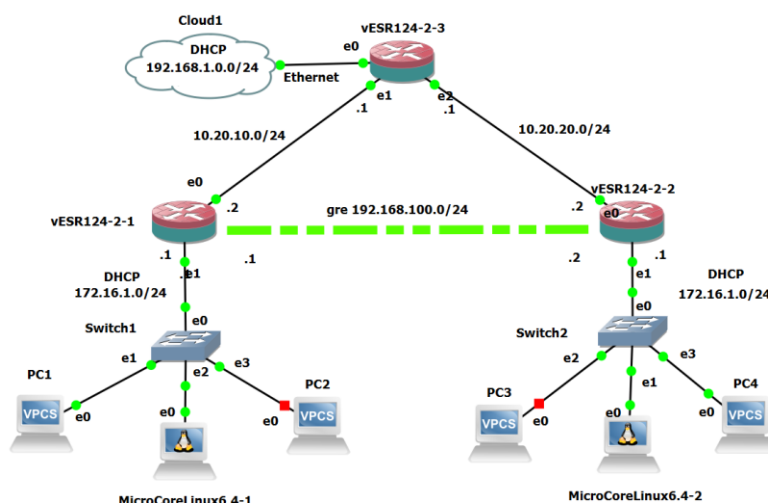


РИСУНОК 8-1. ТОННЕЛЬ GRE.

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*arenda-server.cloud

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.rumcgrp.ru

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). teneu.ruELTEXcm.ru

Также нужно создать политику для IPSec-туннеля, которая указывает список профилей, по которым могут согласовываться узлы. tene.ruELTEXcm.ru

После этого можно создать IPSec-туннель, указав шлюз IKE-протокола, политику IPSec-туннеля, режим обмена ключами и способ установления соединения. tene.ruELTEXcm.ru. 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/docs.eltex-o.rusysahelper.gitbook.io, 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 192.168.1.100/24. На стороне удаленного филиала IP адрес самого туннеля будет 192.168.100.2/24.

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 с 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 туннель. Создадим туннель GRE 10:

```
vesr124-2-1(config)# tunnel gre 10
```

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

```
vesr124-2-1(config-gre)# local address 10.10.10.2
vesr124-2-1(config-gre)# remote address 10.10.20.2
```

Укажем IP-адрес туннеля 192.168.100.1/24:

```
vesr124-2-1(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:

```
vesr124-2-1(config-gre)# security-zone UNTRUSTED
```

Включим туннель:

```
vesr124-2-1(config-gre)# enable  
vesr124-2-1(config-gre)# exit
```

```
vesr-1(config)# tunnel gre 10  
vesr-1(config-gre)# security-zone UNTRUST  
vesr-1(config-gre)# local address 10.10.10.2  
vesr-1(config-gre)# remote address 10.10.20.2  
vesr-1(config-gre)# ip address 192.168.100.1/24  
vesr-1(config-gre)# enable  
vesr-1(config-gre)# exit  
vesr-1(config)#
```

РИСУНОК 8-2. ЭКРАН ТЕРМИНАЛА С КОНФИГУРАЦИЕЙ ТУННЕЛЯ.

Применяем настройки:

```
vesr124-2-1(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
```

```
vesr124-2-1(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
vesr124-2-1(config)#
```

Повторяем эту настройку зеркально для виртуального маршрутизатора vesr124-2-2:

```
vesr124-2-2(config)# tunnel gre 10
```

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

```
vesr124-2-2(config-gre)# local address 10.10.20.2
vesr124-2-2(config-gre)# remote address 10.10.10.20
```

Укажем IP-адрес туннеля 192.168.100.2/24:

```
vesr124-2-2(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:

```
vesr124-2-2(config-gre)# security-zone UNTRUSTED
```

Включим туннель:

```
vesr124-2-2(config-gre)# enable
vesr124-2-2(config-gre)# exit
```

```
vesr-2# config
vesr-2(config)# tunnel gre 10
vesr-2(config-gre)# local address 10.10.20.2
vesr-2(config-gre)# remote address 10.10.10.2
vesr-2(config-gre)# ip address 192.168.100.2/24
vesr-2(config-gre)# security-zone UNTRUST
vesr-2(config-gre)# enable
vesr-2(config-gre)# exit
```

РИСУНОК 8-3. ЭКРАН ТЕРМИНАЛА С КОНФИГУРАЦИЕЙ ТУННЕЛЯ.

Применяем настройки проверяем:

vesr124-2-1# sh ip int				
IP address		Interface	Admin	Link
Type	Precedence			

static	10.10.10.2/24	gi1/0/1	Up	Up
	primary			
static	172.16.1.1/24	gi1/0/2	Up	Up
	primary			
static	192.168.100.1/24	gre 10	Up	Up
	primary			
vesr124-2-1# 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				
vesr124-2-1#				
vesr124-2-2# sh ip int				
IP address		Interface	Admin	Link
Type	Precedence			

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

```

172.16.2.1/24                                gi1/0/2      Up    Up
static primary
192.168.100.2/24                             gre 10       Up    Up
static primary
vesr124-2-2# 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
vesr124-2-2#

```

Туннель поднялся и доступен с обеих сторон.

Важно! Следует разрешить прохождение пакетов протокола GRE через фаерволл на обеих 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 удобства наблюдения за трассой прохождения пакетов IP необходимо разрешить traceroute в фаерволле на обеих сторонах топологии:

Создается группа для сервиса traceroute:

```

vesr124-2-1# config
vesr124-2-1(config)# object-group service TRACEROUTE
vesr124-2-1(config-object-group-service)# port-range 33434-33534
vesr124-2-1(config-object-group-service)# exit

```

И добавляем еще несколько правил в работу файвола:

Для зоны UNTRUST self

```

vesr124-2-1(config)# security zone-pair UNTRUST self
vesr124-2-1(config-security-zone-pair)# rule 3
vesr124-2-1(config-security-zone-pair-rule)# description
"TRACEROUTE"
vesr124-2-1(config-security-zone-pair-rule)# action permit
vesr124-2-1(config-security-zone-pair-rule)# match protocol udp
vesr124-2-1(config-security-zone-pair-rule)# match destination-port
TRACEROUTE
Syntax error: Illegal parameter
vesr124-2-1(config-security-zone-pair-rule)# enable
vesr124-2-1(config-security-zone-pair-rule)# exit
vesr124-2-1(config-security-zone-pair)# exit
vesr124-2-1(config)#
Для зоны UNTRUST TRUST:
vesr124-2-1(config)# security zone-pair UNTRUST TRUST
vesr124-2-1(config-security-zone-pair)# rule 2
vesr124-2-1(config-security-zone-pair-rule)# action permit
vesr124-2-1(config-security-zone-pair-rule)# match protocol udp
vesr124-2-1(config-security-zone-pair-rule)# match destination-
port object-group
TRACEROUTE
vesr124-2-1(config-security-zone-pair-rule)# enable
vesr124-2-1(config-security-zone-pair-rule)# exit
vesr124-2-1(config-security-zone-pair)# exit
vesr124-2-1(config)#

```

Для зоны TRUST UNTRUST:

```

vesr124-2-1(config)# security zone-pair TRUST UNTRUST
vesr124-2-1(config-security-zone-pair)# rule 2
vesr124-2-1(config-security-zone-pair-rule)# action permit
vesr124-2-1(config-security-zone-pair-rule)# match protocol udp
vesr124-2-1(config-security-zone-pair-rule)# match destination-port
object-group

```

TRACEROUTE

```
vesr124-2-1(config-security-zone-pair-rule)# enable
vesr124-2-1(config-security-zone-pair-rule)# exit
vesr124-2-1(config-security-zone-pair)# exit
vesr124-2-1(config)#
```

Для удаленного филиала то же самое настраиваем:

Создается группа для сервиса traceroute:

```
vesr124-2-2# config
vesr124-2-2(config)# object-group service TRACEROUTE
vesr124-2-2(config-object-group-service)# port-range 33434-33534
vesr124-2-2(config-object-group-service)# exit
vesr124-2-2(config)# security zone-pair UNTRUST self
vesr124-2-2(config-security-zone-pair)# rule 3
vesr124-2-2(config-security-zone-pair-rule)# description
"TRACEROUTE"
vesr124-2-2(config-security-zone-pair-rule)# action permit
vesr124-2-2(config-security-zone-pair-rule)# match protocol udp
vesr124-2-2(config-security-zone-pair-rule)# enable
vesr124-2-2(config-security-zone-pair-rule)# exit
vesr124-2-2(config-security-zone-pair)# exit
vesr124-2-2(config)#
```

И добавляем еще несколько правил в работу файвола:

Для зоны UNTRUST self

```
vesr124-2-2(config)# security zone-pair UNTRUST self
vesr124-2-2(config-security-zone-pair)# rule 3
vesr124-2-2(config-security-zone-pair-rule)# description "TRACEROUTE"
vesr124-2-2(config-security-zone-pair-rule)# action permit
vesr124-2-2(config-security-zone-pair-rule)# match protocol udp
vesr124-2-2(config-security-zone-pair-rule)# match destination-port TRACEROUTE
Syntax error: Illegal parameter
vesr124-2-2(config-security-zone-pair-rule)# enable
vesr124-2-2(config-security-zone-pair-rule)# exit
vesr124-2-2(config-security-zone-pair)# exit
vesr124-2-2(config)#
```

Для зоны UNTRUST TRUST:

```
vesr124-2-2(config)# security zone-pair UNTRUST TRUST
vesr124-2-2(config-security-zone-pair)# rule 2
vesr124-2-2(config-security-zone-pair-rule)# action permit
vesr124-2-2(config-security-zone-pair-rule)# match protocol udp
vesr124-2-2(config-security-zone-pair-rule)# match destination-port object-group
TRACEROUTE
vesr124-2-2(config-security-zone-pair-rule)# enable
vesr124-2-2(config-security-zone-pair-rule)# exit
vesr124-2-2(config-security-zone-pair)# exit
vesr124-2-2(config)#
```

Для зоны TRUST UNTRUST:

```
vesr124-2-2(config)# security zone-pair TRUST UNTRUST
vesr124-2-2(config-security-zone-pair)# rule 2
vesr124-2-2(config-security-zone-pair-rule)# action permit
vesr124-2-2(config-security-zone-pair-rule)# match protocol udp
vesr124-2-2(config-security-zone-pair-rule)# match destination-port
object-group
TRACEROUTE
vesr124-2-2(config-security-zone-pair-rule)# enable
vesr124-2-2(config-security-zone-pair-rule)# exit
vesr124-2-2(config-security-zone-pair)# exit
vesr124-2-2(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 :

```
vesr124-2-1(config)# ip route 172.16.2.0/16 tunnel gre 10
```

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

```
vesr124-2-2(config)# ip route 172.16.1.0/16 tunnel gre 10
```

Состояние туннеля можно посмотреть командой:

```
vesr124-2-1# 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: --
vesr124-2-1#
```

```
vesr124-2-2# 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:	--

vesr124-2-2#

Счетчики входящих и отправленных пакетов можно посмотреть командой:

vesr124-2-1# show tunnels counters gre 10

Конфигурацию туннеля можно посмотреть командой:

vesr124-2-1# 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)
```

С 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 PC4 пакеты идут мимо тоннеля по физическому интерфейсу Gi1/0/1 напрямую.

Смотрим конфиг на виртуальном роутере vesr124-2-2 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

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

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/juniper.net/networkengineering.stackexchange.com

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. Сейчас пакеты с данными идут по туннелю в открытом виде, что не рекомендуется. Нужно их зашифровать. Для этого применим протокол шифрования из набора IPSEC.

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:

На роутере vesr124-2-1:

```
security ike proposal ike_prop1
  authentication algorithm md5
  encryption algorithm aes128
  dh-group 2
exit
```

На роутере vesr124-2-2:

```
security ike proposal ike_prop1
  authentication algorithm md5
  encryption algorithm aes128
  dh-group 2
exit
```

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

На роутере vesr124-2-1:

```
security ike policy ike_pol1
  pre-shared-key ascii-text P@ssw0rd
  proposal ike_prop1
exit
```

На роутере vesr124-2-2:

```
security ike policy ike_pol1
  pre-shared-key ascii-text P@ssw0rd
  proposal ike_prop1
exit
```

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

На роутере vesr124-2-1:

```
security ike gateway ike_gw1
  ike-policy ike_pol1
  local address 10.10.10.2
  local network 10.10.10.2/32 protocol gre
  remote address 10.10.20.2
  remote network 10.10.20.2/32 protocol gre
  mode policy-based
exit
```

На роутере vesr124-2-2:

```
security ike gateway ike_gw1
  ike-policy ike_pol1
  local address 10.10.20.2
  local network 10.10.20.2/32 protocol gre
  remote address 10.10.10.2
  remote network 10.10.10.2/32 protocol gre
  mode policy-based
exit
```

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:

На роутере vesr124-2-1:

```
security ipsec proposal ipsec_prop1
  authentication algorithm md5
  encryption algorithm aes128
  pfs dh-group 2
exit
```

На роутере vesr124-2-2:

```
security ipsec proposal ipsec_prop1
```

```
authentication algorithm md5
encryption algorithm aes128
pfs dh-group 2
exit
```

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

На роутере vesr124-2-1:

```
security ipsec policy ipsec_pol1
proposal ipsec_prop1
exit
```

На роутере vesr124-2-2:

```
security ipsec policy ipsec_pol1
proposal ipsec_prop1
exit
```

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.

На роутере vesr124-2-1:

```
security ipsec policy ipsec_pol1
proposal ipsec_prop1
exit
```

На роутере vesr124-2-2:

```
security ipsec policy ipsec_pol1
proposal ipsec_prop1
exit
```

На роутере vesr124-2-1:

```
security ipsec vpn ipsec1
ike establish-tunnel route
```

```
ike gateway ike_gw1
ike ipsec-policy ipsec_pol1
enable
exit
```

На роутере vesr124-2-2:

```
security ipsec vpn ipsec1
ike establish-tunnel route
ike gateway ike_gw1
ike ipsec-policy ipsec_pol1
enable
exit
```

Настраиваем firewall:

На роутере vesr124-2-1:

```
security zone-pair UNTRUST self
rule 4
description "ESP"
action permit
match protocol esp
enable
exit
rule 5
description "AH"
action permit
match protocol ah
enable
exit
exit
```

На роутере vesr124-2-2:

```
security zone-pair UNTRUST self
rule 4
description "ESP"
action permit
match protocol esp
enable
exit
```

```
rule 5
  description "AH"
  action permit
  match protocol ah
  enable
exit
exit
```

Применяем настройки на роутерах:

```
do commit
do confirm
```

Протокол настройки:

На роутере vesr124-2-1:

```
vesr124-2-1# config
vesr124-2-1(config)# security ike proposal ike_prop1
vesr124-2-1(config-ike-proposal)# authentication algorithm md5
vesr124-2-1(config-ike-proposal)# encryption algorithm aes128
vesr124-2-1(config-ike-proposal)# dh-group 2
vesr124-2-1(config-ike-proposal)# exit
vesr124-2-1(config)# security ike policy ike_pol1
vesr124-2-1(config-ike-policy)# pre-shared-key ascii-text P@ssw0rd
vesr124-2-1(config-ike-policy)# proposal ike_prop1
vesr124-2-1(config-ike-policy)# exit
vesr124-2-1(config)# security ike gateway ike_gw1
vesr124-2-1(config-ike-gw)# ike-policy ike_pol1
vesr124-2-1(config-ike-gw)# local address 10.10.10.2
vesr124-2-1(config-ike-gw)# local network 10.10.10.2/32 protocol
gre
vesr124-2-1(config-ike-gw)# remote address 10.10.20.2
vesr124-2-1(config-ike-gw)# remote network 10.10.20.2/32 protocol
gre
vesr124-2-1(config-ike-gw)# mode policy-based
vesr124-2-1(config-ike-gw)# exit
vesr124-2-1(config)# security ipsec proposal ipsec_prop1
vesr124-2-1(config-ipsec-proposal)# authentication algorithm md5
vesr124-2-1(config-ipsec-proposal)# encryption algorithm aes128
vesr124-2-1(config-ipsec-proposal)# pfs dh-group 2
```

```

vesr124-2-1(config-ipsec-proposal)# exit
vesr124-2-1(config)# security ipsec policy ipsec_pol1
vesr124-2-1(config-ipsec-policy)# proposal ipsec_prop1
vesr124-2-1(config-ipsec-policy)# exit
vesr124-2-1(config)# security ipsec vpn ipsec1
vesr124-2-1(config-ipsec-vpn)# ike establish-tunnel route
vesr124-2-1(config-ipsec-vpn)# ike gateway ike_gw1
vesr124-2-1(config-ipsec-vpn)# ike ipsec-policy ipsec_pol1
vesr124-2-1(config-ipsec-vpn)# enable
vesr124-2-1(config-ipsec-vpn)# exit
vesr124-2-1(config)# security zone-pair UNTRUST self
vesr124-2-1(config-security-zone-pair)# rule 4
vesr124-2-1(config-security-zone-pair-rule)# description "ESP"
vesr124-2-1(config-security-zone-pair-rule)# action permit
vesr124-2-1(config-security-zone-pair-rule)# match protocol esp
vesr124-2-1(config-security-zone-pair-rule)# enable
vesr124-2-1(config-security-zone-pair-rule)# exit
vesr124-2-1(config-security-zone-pair)# rule 5
vesr124-2-1(config-security-zone-pair-rule)# description "AH"
vesr124-2-1(config-security-zone-pair-rule)# action permit
vesr124-2-1(config-security-zone-pair-rule)# match protocol ah
vesr124-2-1(config-security-zone-pair-rule)# enable
vesr124-2-1(config-security-zone-pair-rule)# exit
vesr124-2-1(config-security-zone-pair)# exit
vesr124-2-1(config)# do commit

```

Configuration has been successfully applied and saved to flash.

Commit timer started, changes will be reverted in 600 seconds.

2025-06-25T16:00:49+00:00 %CLI-I-CRIT: user admin from console
input: do commit

```
vesr124-2-1(config)# do confirm
```

Configuration has been confirmed. Commit timer canceled.

2025-06-25T16:00:54+00:00 %CLI-I-CRIT: user admin from console
input: do confirm

```
vesr124-2-1(config)# exit
```

```
vesr124-2-1#
```

На поутере vesr124-2-2:

```

vesr124-2-2# config
vesr124-2-2(config)# security ike proposal ike_prop1
vesr124-2-2(config-ike-proposal)# authentication algorithm md5
vesr124-2-2(config-ike-proposal)# encryption algorithm aes128

```

```

vesr124-2-2(config-ike-proposal)# dh-group 2
vesr124-2-2(config-ike-proposal)# exit
vesr124-2-2(config)# security ike policy ike_pol1
vesr124-2-2(config-ike-policy)# pre-shared-key ascii-text P@ssw0rd
vesr124-2-2(config-ike-policy)# proposal ike_prop1
vesr124-2-2(config-ike-policy)# exit
vesr124-2-2(config)# security ike gateway ike_gw1
vesr124-2-2(config-ike-gw)# ike-policy ike_pol1
vesr124-2-2(config-ike-gw)# local address 10.10.20.2
vesr124-2-2(config-ike-gw)# local network 10.10.20.2/32 protocol
gre
vesr124-2-2(config-ike-gw)# remote address 10.10.10.2
vesr124-2-2(config-ike-gw)# remote network 10.10.10.2/32 protocol
gre
vesr124-2-2(config-ike-gw)# mode policy-based
vesr124-2-2(config-ike-gw)# exit
vesr124-2-2(config)# security ipsec proposal ipsec_prop1
vesr124-2-2(config-ipsec-proposal)# authentication algorithm md5
vesr124-2-2(config-ipsec-proposal)# encryption algorithm aes128
vesr124-2-2(config-ipsec-proposal)# pfs dh-group 2
vesr124-2-2(config-ipsec-proposal)# exit
vesr124-2-2(config)# security ipsec policy ipsec_pol1
vesr124-2-2(config-ipsec-policy)# proposal ipsec_prop1
vesr124-2-2(config-ipsec-policy)# exit
vesr124-2-2(config)# security ipsec vpn ipsec1
vesr124-2-2(config-ipsec-vpn)# ike establish-tunnel route
vesr124-2-2(config-ipsec-vpn)# ike gateway ike_gw1
vesr124-2-2(config-ipsec-vpn)# ike ipsec-policy ipsec_pol1
vesr124-2-2(config-ipsec-vpn)# enable
vesr124-2-2(config-ipsec-vpn)# exit
vesr124-2-2(config)# security zone-pair UNTRUST self
vesr124-2-2(config-security-zone-pair)# rule 4
vesr124-2-2(config-security-zone-pair-rule)# description "ESP"
vesr124-2-2(config-security-zone-pair-rule)# action permit
vesr124-2-2(config-security-zone-pair-rule)# match protocol esp
vesr124-2-2(config-security-zone-pair-rule)# enable
vesr124-2-2(config-security-zone-pair-rule)# exit
vesr124-2-2(config-security-zone-pair)# rule 5
vesr124-2-2(config-security-zone-pair-rule)# description "AH"
vesr124-2-2(config-security-zone-pair-rule)# action permit
vesr124-2-2(config-security-zone-pair-rule)# match protocol ah
vesr124-2-2(config-security-zone-pair-rule)# enable

```

```

vesr124-2-2(config-security-zone-pair-rule)# exit
vesr124-2-2(config-security-zone-pair)# exit
vesr124-2-2(config)# do commit
Configuration has been successfully applied and saved to flash.
Commit timer started, changes will be reverted in 600 seconds.
2025-06-25T16:01:02+00:00 %CLI-I-CRIT: user admin from console
input: do commit
vesr124-2-2(config)# do confirm
Configuration has been confirmed. Commit timer canceled.
2025-06-25T16:01:06+00:00 %CLI-I-CRIT: user admin from console
input: do confirm
vesr124-2-2(config)# exit
vesr124-2-2#

```

Проверяем на роутере vesr124-2-1:

```

vesr124-2-1# sh security ipsec vpn configuration
Name           Description           State
-----
ipsec1         --                   Enabled
vesr124-2-1# sh security ipsec vpn configuration ipsec1
VRF:           --
Description:    --
State:          Enabled
IKE:
  Establish tunnel:  route
  IPsec policy:      ipsec_pol1
  IKE gateway:       ike_gw1
  IKE DSCP:          63
  IKE idle-time:     0s
  IKE rekeying:      Enabled
    Margin time:      540s
    Margin kilobytes: 0
    Margin packets:   0
    Randomization:    100%
vesr124-2-1#

```

Проверяем на роутере vesr124-2-2:

```

vesr124-2-2# sh security ipsec vpn configuration
Name           Description           State
-----

```

```

ipsec1          --          Enabled
vesr124-2-2# sh security ipsec vpn configuration ipsec1
VRF:            --
Description:    --
State:          Enabled
IKE:
  Establish tunnel:  route
  IPsec policy:      ipsec_pol1
  IKE gateway:       ike_gw1
  IKE DSCP:          63
  IKE idle-time:     0s
  IKE rekeying:      Enabled
    Margin time:     540s
    Margin kilobytes: 0
    Margin packets:  0
    Randomization:   100%
vesr124-2-2#

```

Проверка состояния vpn на обоих роутерах:

```

vesr124-2-1# sh security ipsec vpn status
vesr124-2-1#

```

Ничего нету. Потому , что для инициализации необходимо, что бы в туннель начали приходить пакеты, для этого запустим трассу:

```

gns3@box:~$ traceroute 172.16.2.2
traceroute to 172.16.2.2 (172.16.2.2), 30 hops max, 38 byte packets
 1 172.16.1.1 (172.16.1.1) 15.253 ms 1.213 ms 1.220 ms
 2 192.168.100.2 (192.168.100.2) 2.595 ms 16.045 ms 4.787 ms
 3 172.16.2.2 (172.16.2.2) 26.368 ms 3.358 ms 3.142 ms
gns3@box:~$

```

И проверяем еще раз:

```

vesr124-2-1# sh security ipsec vpn status
Name          Local host  Remote host  Initiator spi
Responder spi  State
-----
-----

```

```
ipsec1          10.10.10.2    10.10.20.2
0x480615bbe0f088db 0x43d74dcb9ac0c174 Established
```

```
vesr124-2-2# sh security ipsec vpn status
Name                Local host    Remote host    Initiator spi
Responder spi      State
-----
```

```
ipsec1          10.10.20.2    10.10.10.2
0x480615bbe0f088db 0x43d74dcb9ac0c174 Established
```

Есть прохождение пакетов в туннеле и они зашифрованы:

```
gns3@box:~$ traceroute 172.16.2.2
traceroute to 172.16.2.2 (172.16.2.2), 30 hops max, 38 byte packets
 1 172.16.1.1 (172.16.1.1) 15.253 ms 1.213 ms 1.220 ms
 2 192.168.100.2 (192.168.100.2) 2.595 ms 16.045 ms 4.787 ms
 3 172.16.2.2 (172.16.2.2) 26.368 ms 3.358 ms 3.142 ms
gns3@box:~$
```

```
gns3@box:~$ traceroute 172.16.1.2
traceroute to 172.16.1.2 (172.16.1.2), 30 hops max, 38 byte packets
 1 172.16.2.1 (172.16.2.1) 1.406 ms 0.918 ms 0.885 ms
 2 192.168.100.1 (192.168.100.1) 2.926 ms 1.823 ms 1.618 ms
 3 172.16.1.2 (172.16.1.2) 3.928 ms 2.580 ms 0.777 ms
gns3@box:~$
```

Конфигурация устройств получилась следующая:

```
hostname vesr124-2-1

object-group service dhcp_service
  port-range 67
exit
object-group service dhcp_client
  port-range 68
exit
object-group service ssh
  port-range 22
exit
object-group service SSH
```

```
    port-range 2222
  exit
  object-group service TRACEROUTE
    port-range 33434-33534
  exit

  object-group network WAN
    ip address-range 10.10.10.2
  exit
  object-group network clients
    ip address-range 192.168.10.0-192.168.10.254
    ip address-range 192.168.151.1-192.168.151.254
    ip address-range 10.10.10.1-10.10.10.254
    ip address-range 10.10.20.1-10.10.20.254
    ip address-range 172.16.2.1-172.16.2.254
  exit
  object-group network SERVER_IP
    ip address-range 172.16.1.2
  exit
  object-group network LAN_NETWORK
    ip address-range 172.16.1.1-172.16.1.254
  exit
  object-group network LAN_GW
    ip address-range 172.16.1.1
  exit

  syslog max-files 3
  syslog file-size 512
  syslog file tmpsys:syslog/default
    severity info
  exit
  syslog console
    virtual-serial
  exit

  username admin
    password encrypted
$6$Kx1jB3DT6zH05CQ7$WqbKGSvl/35jvx.NKDc6R5NpD5uy2623zfbWAO
TPhNOQgnR.zXxQzlgYwESdbOXOWSyhPPNojy0Q0.pMvR6Ld/
  exit
  username rinat
```

```
password encrypted
$6$T37FYJy.i38S36O0$vHt9c.g0yzphZ5PJNwkmOvJJ36dSvMbr7qRSJnDWh
prk4f8OI5d1oNdT6jmqUsXMbfgRFDd4RK3Ugeu0jLZ9w/
privilege 15
exit

domain lookup enable

security zone UNTRUST
exit
security zone TRUST
exit

interface gigabitethernet 1/0/1
description "WAN"
security-zone UNTRUST
ip address 10.10.10.2/24
exit
interface gigabitethernet 1/0/2
description "LAN_NET"
security-zone TRUST
ip address 172.16.1.1/24
exit
interface gigabitethernet 1/0/3
shutdown
ip address dhcp
exit

tunnel gre 10
ttl 18
security-zone UNTRUST
local address 10.10.10.2
remote address 10.10.20.2
ip address 192.168.100.1/24
enable
exit

security zone-pair TRUST self
rule 1
description "ICMP"
action permit
match protocol icmp
```

```
    enable
exit
rule 2
    action permit
    match protocol udp
    enable
exit
rule 3
    description "GRE"
    action permit
    match protocol gre
    enable
exit
rule 4
    action permit
    match protocol udp
    match source-port object-group dhcp_client
    match destination-port object-group dhcp_service
    enable
exit
exit
security zone-pair TRUST UNTRUST
rule 1
    action permit
    match protocol icmp
    enable
exit
rule 2
    action permit
    match protocol udp
    enable
exit
rule 3
    description "GRE"
    action permit
    match protocol gre
    enable
exit
exit
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
rule 3
    description "TRACEROUTE"
    action permit
    match protocol udp
    enable
exit
rule 4
    description "ESP"
    action permit
    match protocol esp
    enable
exit
rule 5
    description "AH"
    action permit
    match protocol ah
    enable
exit
rule 10
    action permit
    match protocol tcp
    match source-address object-group clients
    match destination-address object-group WAN
    match destination-port object-group ssh
    enable
exit
exit
security zone-pair UNTRUST TRUST
rule 1
    description "ICMP"
    action permit
    match protocol icmp
```

```
    enable
exit
rule 2
    description "GRE"
    action permit
    match protocol gre
    enable
exit
rule 3
    description "TRACEROUTE"
    action permit
    match protocol udp
    enable
exit
rule 10
    action permit
    match protocol tcp
    match destination-address object-group SERVER_IP
    enable
exit
exit

security ike proposal ike_prop1
    authentication algorithm md5
    encryption algorithm aes128
    dh-group 2
exit

security ike policy ike_pol1
    pre-shared-key ascii-text encrypted AC94107EA75F5AFF
    proposal ike_prop1
exit

security ike gateway ike_gw1
    ike-policy ike_pol1
    local address 10.10.10.2
    local network 10.10.10.2/32 protocol gre
    remote address 10.10.20.2
    remote network 10.10.20.2/32 protocol gre
    mode policy-based
exit
```

```
security ipsec proposal ipsec_prop1
  authentication algorithm md5
  encryption algorithm aes128
  pfs dh-group 2
exit
```

```
security ipsec policy ipsec_pol1
  proposal ipsec_prop1
exit
```

```
security ipsec vpn ipsec1
  ike establish-tunnel route
  ike gateway ike_gw1
  ike ipsec-policy ipsec_pol1
  enable
exit
```

```
security passwords default-expired
```

```
nat destination
  pool SERVER_POOL
  ip address 172.16.1.2
  ip port 22
exit
ruleset DNAT
  from zone UNTRUST
  rule 10
    match protocol tcp
    match destination-port object-group SSH
    action destination-nat pool SERVER_POOL
    enable
  exit
exit
exit
```

```
nat source
  pool WAN
  ip address-range 10.10.10.2
  exit
ruleset SNAT
  to zone UNTRUST
  rule 1
```

```
match source-address object-group LAN_NETWORK
action source-nat interface
enable
exit
exit
exit
```

```
ip dhcp-server
ip dhcp-server pool LAN_NETWORK
network 172.16.1.0/24
default-lease-time 003:00:00
address-range 172.16.1.1-172.16.1.254
address 172.16.1.2 mac-address 0c:28:d9:73:00:00
default-router 172.16.1.1
dns-server 77.88.8.8
exit
```

```
ip route 0.0.0.0/0 10.10.10.1
ip route 10.10.20.0/24 10.10.20.1
ip route 10.10.30.0/24 10.10.30.1
ip route 172.16.2.0/24 tunnel gre 10
ip route 172.16.1.0/24 interface gigabitethernet 1/0/2
```

```
ip ssh server
```

```
ntp enable
ntp broadcast-client enable
```

```
licence-manager
host address elm.eltex-co.ru
exit
```

```
hostname vesr124-2-2
```

```
object-group service dhcp_service
port-range 67
exit
object-group service dhcp_client
port-range 68
exit
object-group service TRACEROUTE
```

```
port-range 33434-33534
exit
```

```
object-group network LAN_NETWORK
  ip address-range 172.16.2.1-172.16.2.254
exit
object-group network LAN_GW
  ip address-range 172.16.2.1
exit
object-group network WAN
  ip address-range 10.10.20.2
exit
object-group network clients
  ip address-range 192.168.10.0-192.168.10.254
  ip address-range 192.168.151.1-192.168.151.254
  ip address-range 10.10.10.1-10.10.10.254
  ip address-range 10.10.20.1-10.10.20.254
  ip address-range 172.16.1.0-172.16.2.254
exit
```

```
syslog max-files 3
syslog file-size 512
syslog file tmpsys:syslog/default
  severity info
exit
syslog console
  virtual-serial
exit
```

```
username admin
  password encrypted
$6$IB0aLOlcTz4bCj3C$.wb4QEOgQALUdzELWRMrUsSm3qP31ijGHFq6p7
rtnZtaPiwTLb5Y2N7dt9fvK/aNIULZ1yEzK6CM5u0uMiNtn/
exit
```

```
domain lookup enable
```

```
security zone TRUST
exit
security zone UNTRUST
exit
```

```
interface gigabitethernet 1/0/1
  description "WAN"
  security-zone UNTRUST
  ip address 10.10.20.2/24
exit
interface gigabitethernet 1/0/2
  description "LAN"
  security-zone TRUST
  ip address 172.16.2.1/24
exit

tunnel gre 10
  ttl 18
  security-zone UNTRUST
  local address 10.10.20.2
  remote address 10.10.10.2
  ip address 192.168.100.2/24
  enable
exit

security zone-pair TRUST self
  rule 1
    description "ICMP"
    action permit
    match protocol icmp
    enable
  exit
  rule 2
    description "GRE"
    action permit
    match protocol gre
    enable
  exit
  rule 3
    description "TRACEROUTE"
    action permit
    match protocol udp
    enable
  exit
  rule 4
    action permit
    match protocol udp
```

```
    match source-port object-group dhcp_client
    match destination-port object-group dhcp_service
    enable
exit
exit
security zone-pair TRUST UNTRUST
rule 1
    description "ICMP"
    action permit
    match protocol icmp
    enable
exit
rule 2
    description "GRE"
    action permit
    match protocol gre
    enable
exit
rule 3
    description "TRACEROUTE"
    action permit
    match protocol udp
    enable
exit
exit
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
rule 3
    description "TRACEROUTE"
    action permit
    match protocol udp
```

```
    enable
  exit
rule 4
  description "ESP"
  action permit
  match protocol esp
  enable
exit
rule 5
  description "AH"
  action permit
  match protocol ah
  enable
exit
exit
security zone-pair UNTRUST TRUST
rule 1
  description "ICMP"
  action permit
  match protocol icmp
  enable
exit
rule 2
  description "GRE"
  action permit
  match protocol gre
  enable
exit
rule 3
  description "TRACEROUTE"
  action permit
  match protocol udp
  enable
exit
rule 10
  action permit
  match protocol tcp
  enable
exit
exit

security ike proposal ike_prop1
```

```
authentication algorithm md5
encryption algorithm aes128
dh-group 2
exit
```

```
security ike policy ike_pol1
pre-shared-key ascii-text encrypted AC94107EA75F5AFF
proposal ike_prop1
exit
```

```
security ike gateway ike_gw1
ike-policy ike_pol1
local address 10.10.20.2
local network 10.10.20.2/32 protocol gre
remote address 10.10.10.2
remote network 10.10.10.2/32 protocol gre
mode policy-based
exit
```

```
security ipsec proposal ipsec_prop1
authentication algorithm md5
encryption algorithm aes128
pfs dh-group 2
exit
```

```
security ipsec policy ipsec_pol1
proposal ipsec_prop1
exit
```

```
security ipsec vpn ipsec1
ike establish-tunnel route
ike gateway ike_gw1
ike ipsec-policy ipsec_pol1
enable
exit
```

```
security passwords default-expired
```

```
nat source
pool WAN
ip address-range 10.10.10.2
exit
```

```
ruleset SNAT
  to zone UNTRUST
  rule 1
    match source-address object-group LAN_NETWORK
    action source-nat interface
    enable
  exit
exit
exit

ip dhcp-server
ip dhcp-server pool LAN_NETWORK
  network 172.16.2.0/24
  default-lease-time 003:00:00
  address-range 172.16.2.1-172.16.2.254
  excluded-address-range 172.16.2.1,172.16.2.254
  default-router 172.16.2.1
  dns-server 77.88.8.8
exit

ip route 0.0.0.0/0 10.10.20.1
ip route 10.10.10.0/24 10.10.10.1
ip route 10.10.30.0/24 10.10.30.1
ip route 172.16.1.0/24 tunnel gre 10
ip route 172.16.2.0/24 interface gigabitethernet 1/0/2

ip ssh server

ntp enable
ntp broadcast-client enable

licence-manager
  host address elm.eltex-co.ru
exit
```

ВЫВОДЫ ПО ГЛАВЕ

- Создан GRE-туннель между двумя офисами через Интернет.
- Исправлены ошибки NAT, влияющие на туннелирование.
- Внедрено шифрование IPSEC.
- Обеспечена маршрутизация и безопасность.

В следующей главе будет рассмотрена схема подключения второго филиала с настройкой туннеля gre+ipsec к центральному офису. Настройка доступа к сервису web httpd сервера.

Глава 9. Настройка нескольких филиалов с на виртуальных маршрутизаторах vESR.

Цель этой работы:

- Запустить WEB сервис в центральном офисе и дать возможность работать с ним в новом втором филиале.
- Создать еще одну локальную сеть во втором филиале.
- Подключить её к интернет.
- Построить защищённый туннель между центральным офисом и вторым филиалом.

Создаём WEB сервер. Для этого устанавливаем сервер HTTPD на машине MicroCoreLinux6.4-1:

```
gns3@box:~$ tce-load -iw busybox-httpd
Downloading: busybox-httpd.tcz
Connecting to repo.tinycorelinux.net (128.127.66.77:80)
busybox-httpd.tcz 100% |*****| 20480
0:00:00 ETA
busybox-httpd.tcz: OK
gns3@box:~$
```

Затем создадим файл с именем *index.html* в нашей папке /home/gns3 со следующим содержимым:

```
<!doctype html>
<html lang="ru-RU">
<html>
  <head>
    <meta charset="utf-8"
    <title>Нью-Васюки->Арбатов</title>
  </head>
  <body>
```

```
<br> Ударим автопробегом по бездорожью, разгильдяйству и  
пофигизму!
```

```
</body>
```

```
</html>
```

Для демонстрации, **во всех следующих примерах** запустим сервер в папке **\$HOME/gns3** для демонстрации **через порт 80**.

Сервер httpd запускается командой:

```
gns3@box:~$ sudo /usr/local/httpd/sbin/httpd -p 80 -h /home/gns3/
```

Проверка что сервис работает делается командой:

```
gns3@box:~$ sudo /usr/local/httpd/sbin/httpd -p 80 -h /home/gns3/
gns3@box:~$ netstat -tuln | grep 80
tcp      0      0 0.0.0.0:80          0.0.0.0:*          LISTEN
```

Для работы с WEB сервером нужен браузер. Это можно сделать по официальному руководству по установке шаблонов (templates) в GNS3- оно доступно на сайте **docs.gns3.com**. На странице «Install an appliance from the GNS3 Marketplace» объясняется, как загружать и устанавливать шаблоны из Marketplace GNS3. Процесс похож для разных операционных систем: Windows, Mac OS и Linux. docs.gns3.com Шаблоны — это JSON-файлы с расширением gns3a. Можно использовать готовые шаблоны из Marketplace или создавать свои. Либо по шагам ниже:

Установим эмулятор браузера непосредственно с сайта GNS3:

Нажимаем левой кнопкой мыши на иконку All devices и потом на -> New template. Как на Рис 9-1.

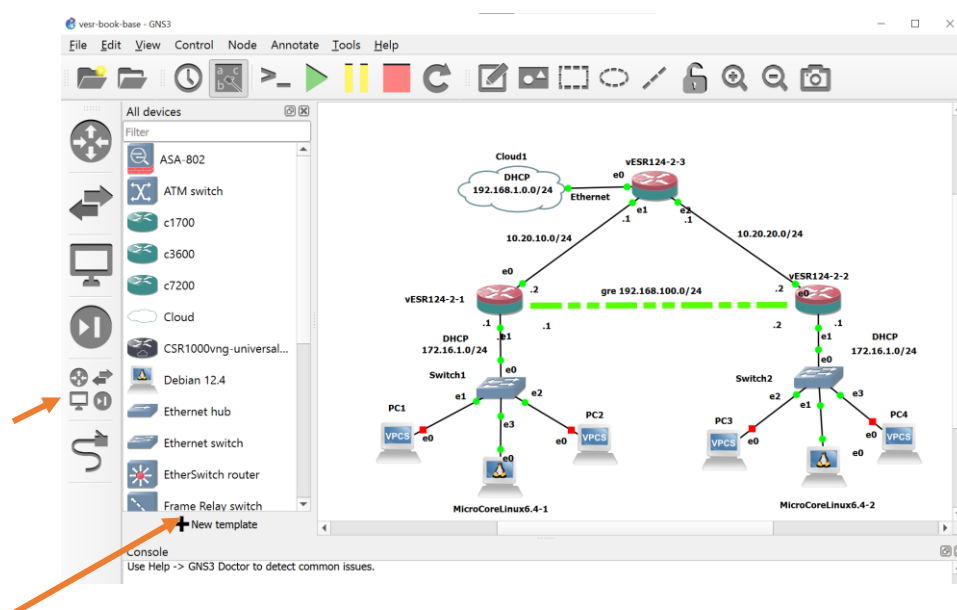


РИСУНОК 9-1. ЭКРАН ВЫБОРА НОВОГО УСТРОЙСТВА.

Появится экран выбора места откуда будет загружаться программа нового устройства с браузером.

New template

New template

Please select how you want to create a new template

- ☒ Install an appliance from the GNS3 server (recommended)
- ☐ Import an appliance file (.gns3a extension)
- ☐ Manually create a new template

РИСУНОК 9-2. ЭКРАН ВЫБОРА МЕСТА ЗАГРУЗКИ.

Нажать “Install” оставив выбор как на экране.

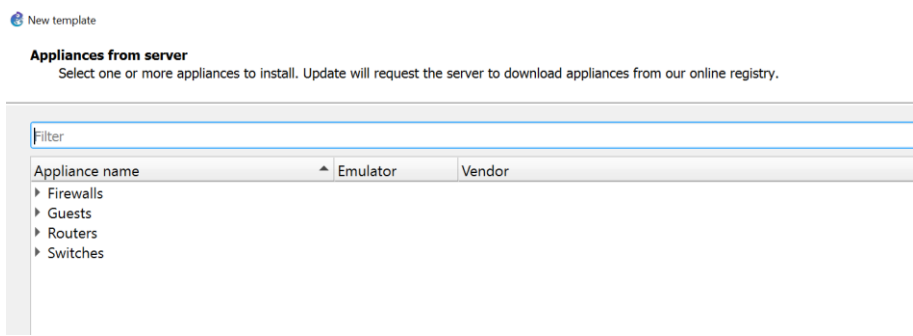


РИСУНОК 9-3. ЭКРАН ВЫБОРА СПИСКА ГОСТЕВЫХ ОБРАЗОВ ВИРТУАЛОК.

Выбрать строчку “Guest” для раскрытия списка.

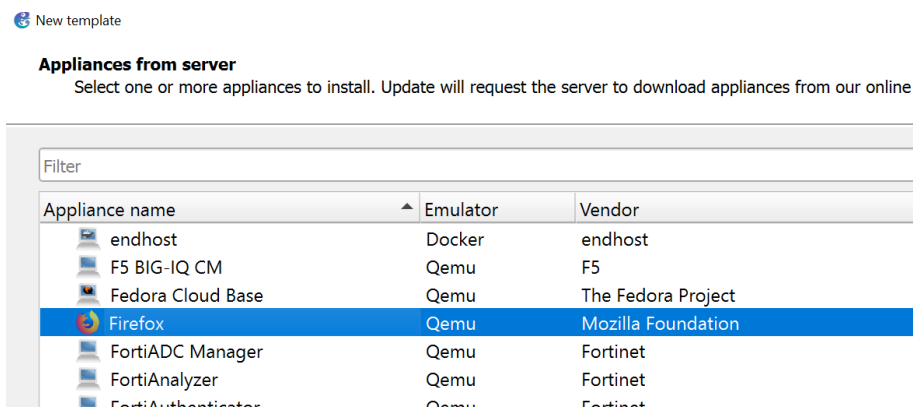


РИСУНОК 9-4. ЭКРАН ВЫБОРА БРАУЗЕРА В ДОКЕРЕ.

Из списка выбрать “Firefox” и нажать “Install”.

Лабораторные работы с виртуальным сервисным маршрутизатором vESR
В графическом симуляторе GNS3

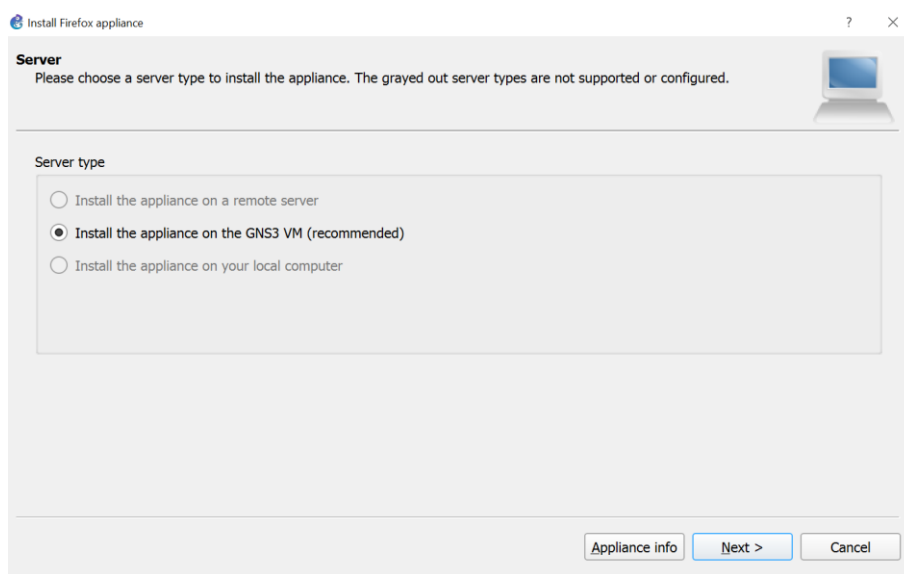


РИСУНОК 9-5. ЭКРАН УСТАНОВКИ.

Здесь просто нажать “Next”.

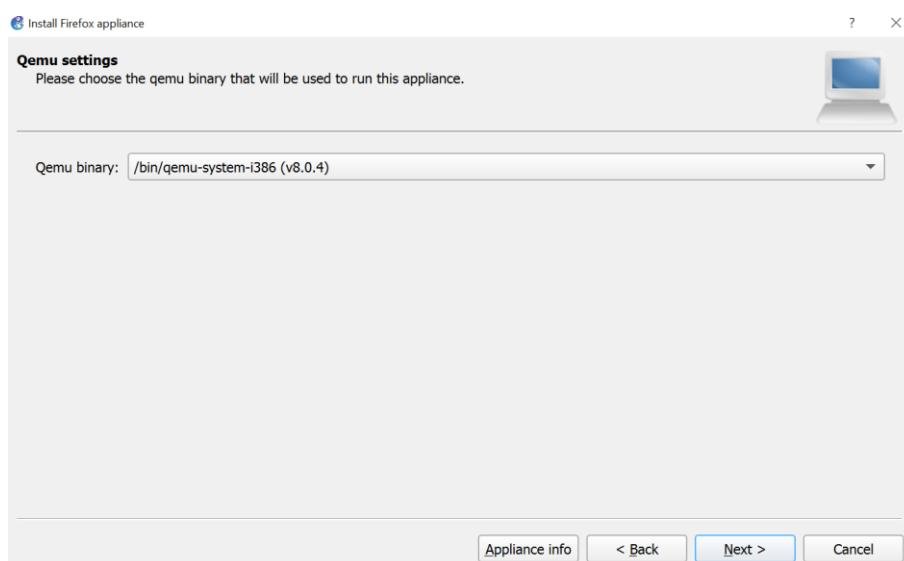


РИСУНОК 9-6. ЭКРАН УСТАНОВКИ.

Нажать еще раз “Next”.

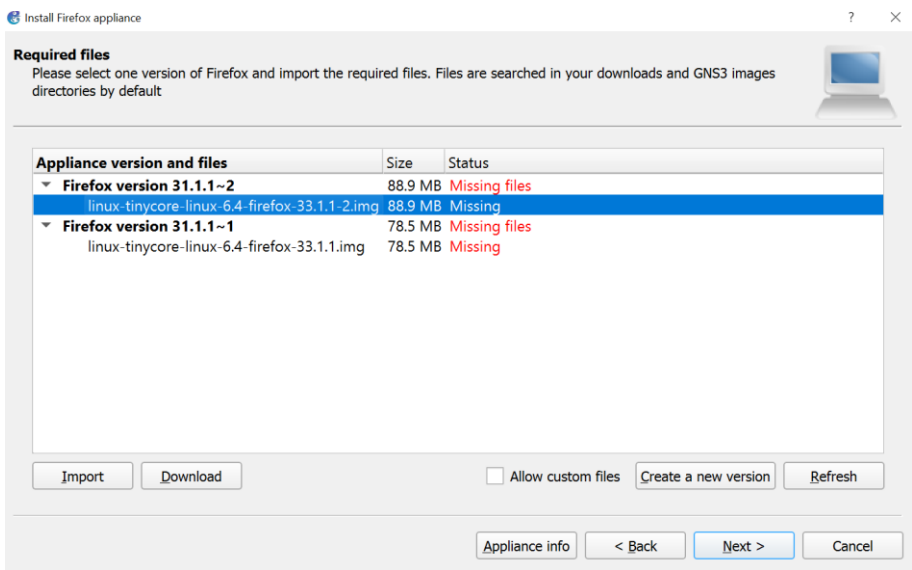


РИСУНОК 9-7. ЭКРАН ВЫБОРА ВАРИАНТА.

Раскрыть верхнюю строчку с названием и нажать на “Dowload” для загрузки образа docker.

По окончании загрузки нажать на кнопку “Refresh” – окно обновится :

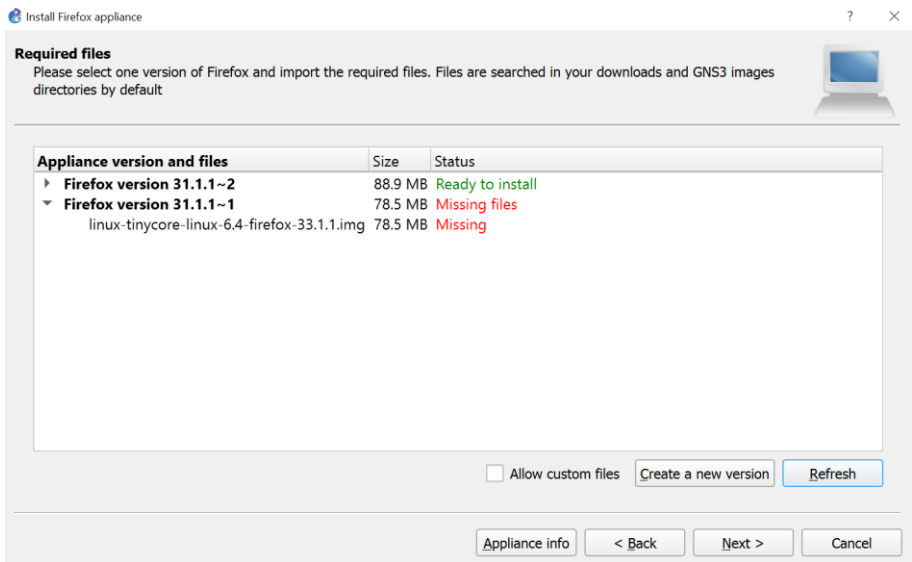


РИСУНОК 9-8. ЭКРАН ЗАГРУЗКИ.

Лабораторные работы с виртуальным сервисным маршрутизатором vESR
В графическом симуляторе GNS3

Выбрать мышью строчку с надписью “Ready to install” далее нажать кнопку “Next”:

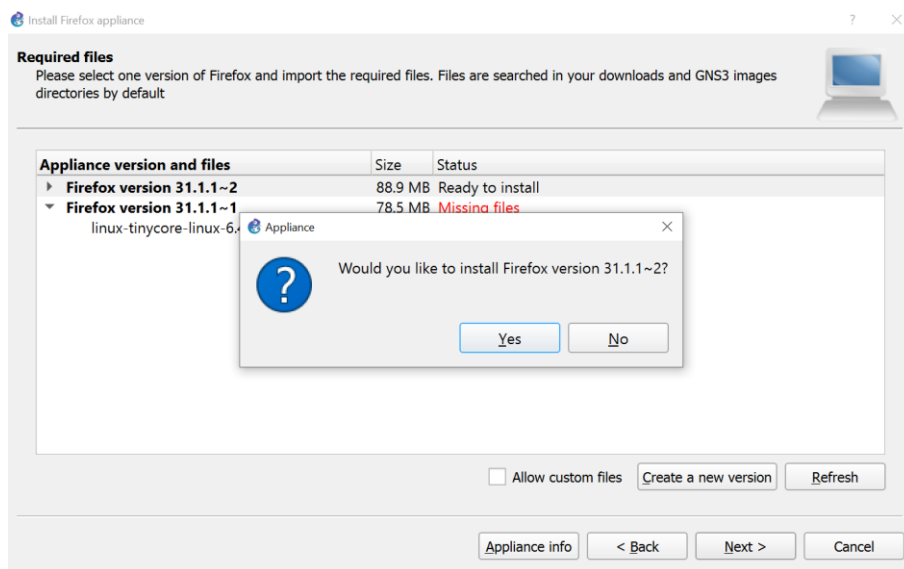


РИСУНОК 9-9. ЭКРАН УСТАНОВКИ.

Нажать кнопку “Yes” и “Finish”.

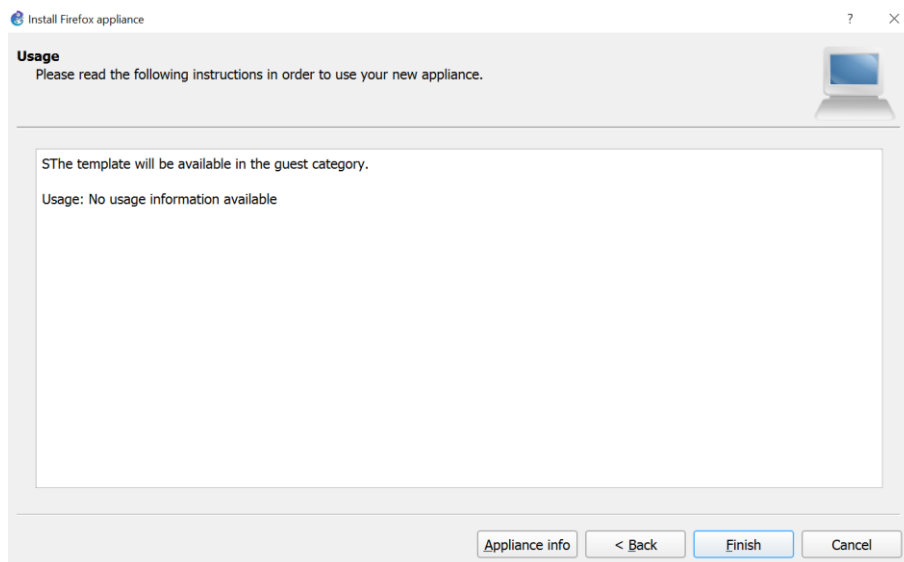


РИСУНОК 9-10. УСТАНОВКА ЗАВЕРШЕНА.

У на экране с встроенными устройствами появится новое устройство – браузер, который можно использовать в схеме для работы.

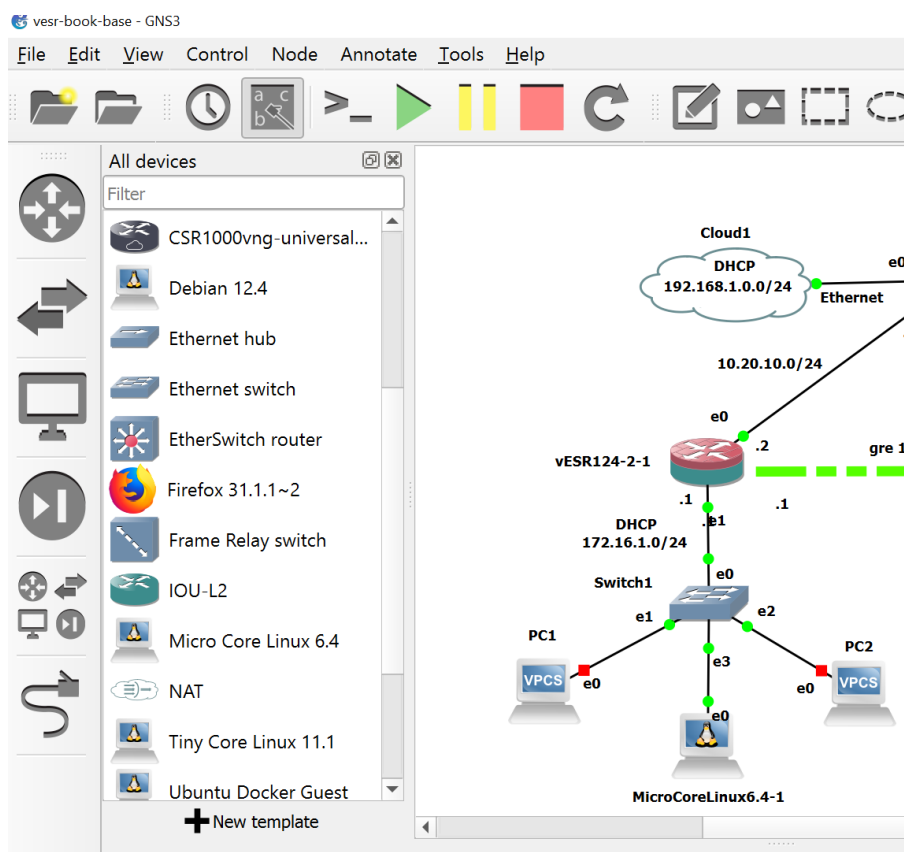


Рисунок 9-11. ЭКРАН С УСТАНОВЛЕННЫМ УСТРОЙСТВОМ С БРАУЗЕРОМ.

Создание нового подключения сети второго филиала делается по той же методике, что и в случае с первым филиалом. Повторите шаги, описанные в главах с 3 по 6 для получения новой конфигурации за исключением настройки Р адресов. На новой схеме добавится устройство с браузером, как показано на Рис 9-12.

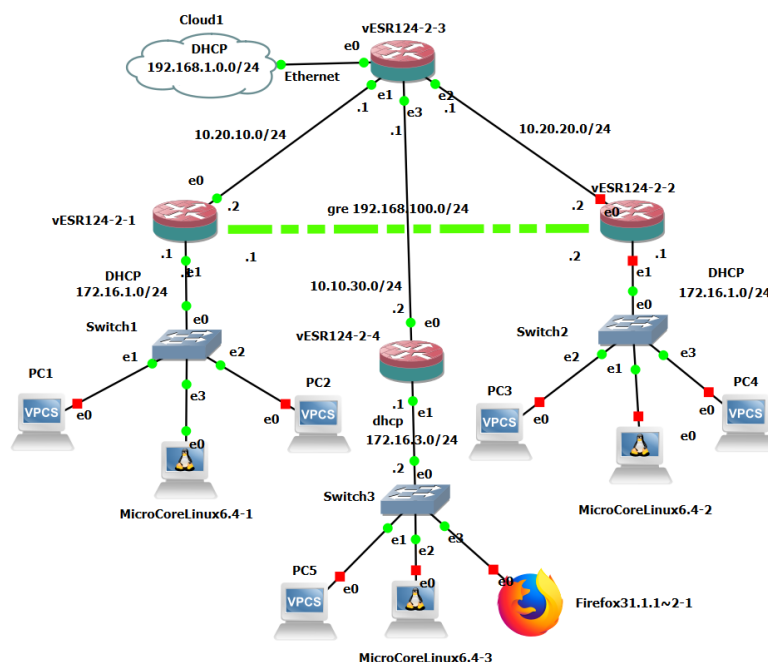


РИСУНОК 9-12. СХЕМА ПОДКЛЮЧЕНИЯ ВТОРОГО ФИЛИАЛА.

Для работы с новой схемой необходимо дополнительно настроить роутеры:

- VESr124-2-1
- VESr124-2-3
- VESr124-2-4

На первом маршрутизаторе необходимо добавить маршрут к новому филиалу, создать зашифрованный туннель gre+ipsec к нему и разрешить прохождение пакетов к порту 80 между зонами UNTRUST и TRUST.

```
vesr124-2-1# config
vesr124-2-1(config)# ip route 10.10.30.0/24 10.10.30.1
vesr124-2-1(config)# ip route 172.16.3.0/24 tunnel gre 3
```

Настраивается новый туннель ко второму филиалу:

```
vesr124-2-1# config
vesr124-2-1(config)# tunnel gre 3
```

```
vesr124-2-1(config-gre)# security-zone UNTRUST
vesr124-2-1(config-gre)# local address 10.10.10.2
vesr124-2-1(config-gre)# remote address 10.10.30.2
vesr124-2-1(config-gre)# ip address 192.168.200.1/24
vesr124-2-1(config-gre)# enable
vesr124-2-1(config-gre)# exit
vesr124-2-1(config)# exit
vesr124-2-1#
```

В конфиге уже есть один настроенный и работающий туннель gre_ipsec с предложениями и политиками по обмену ключами ike:

```
vesr124-2-1# sh run security ike
security ike proposal ike_prop1
  authentication algorithm md5
  encryption algorithm aes128
  dh-group 2
exit
security ike policy ike_pol1
  pre-shared-key ascii-text encrypted AC94107EA75F5AFF
  proposal ike_prop1
exit

security ike gateway ike_gw1
  ike-policy ike_pol1
  local address 10.10.10.2
  local network 10.10.10.2/32 protocol gre
  remote address 10.10.20.2
  remote network 10.10.20.2/32 protocol gre
  mode policy-based
exit
```

и политиками с предложениями ipsec с vpn к нему:

```
vesr124-2-1# sh run security ipsec
security ipsec proposal ipsec_prop1
  authentication algorithm md5
  encryption algorithm aes128
```

```
pfs dh-group 2
exit

security ipsec policy ipsec_pol1
  proposal ipsec_prop1
exit

security ipsec vpn ipsec1
  ike establish-tunnel route
  ike gateway ike_gw1
  ike ipsec-policy ipsec_pol1
  enable
exit
```

Предложения по обмену и политики оставим такие же, добавлять ещё одни, специально к новому туннелю не нужно. Создадим только сами роуты и vpn:

```
vesr124-2-1#
vesr124-2-1# config
vesr124-2-1(config)# security ike gateway ike_gw2
vesr124-2-1(config-ike-gw)# ike-policy ike_pol1
vesr124-2-1(config-ike-gw)# local address 10.10.10.2
vesr124-2-1(config-ike-gw)# local network 10.10.10.2/32 protocol gre
vesr124-2-1(config-ike-gw)# remote address 10.10.30.2
vesr124-2-1(config-ike-gw)# remote network 10.10.30.2/32 protocol gre
vesr124-2-1(config-ike-gw)# mode policy-based
vesr124-2-1(config-ike-gw)# exit
vesr124-2-1(config)# security ipsec vpn ipsec2
vesr124-2-1(config-ipsec-vpn)# ike establish-tunnel route
vesr124-2-1(config-ipsec-vpn)# ike gateway ike_gw2
vesr124-2-1(config-ipsec-vpn)# ike ipsec-policy ipsec_pol1
vesr124-2-1(config-ipsec-vpn)# enable
vesr124-2-1(config-ipsec-vpn)# exit
vesr124-2-1(config)# exit
vesr124-2-1# commit
Nothing to commit in configuration
2025-06-28T16:58:02+00:00 %CLI-I-CRIT: user admin from console
input: commit
```

```
vesr124-2-1# confirm
Nothing to confirm in configuration. You must commit some changes
first.
2025-06-28T16:58:05+00:00 %CLI-I-CRIT: user admin from console
input: confirm
vesr124-2-1#
```

Изменения в конфигурации роутера Vesr124-2-3 сводится к созданию адреса новой сети на интерфейсе. Добавляется сеть 10.10.30.0/24 с адресом 10.10.30.1 на интерфейсе gi1/0/4 для роутера vesr124-2-3:

```
vesr124-2-3#config
vesr124-2-3(config)#
vesr124-2-3(config)# interface gigabitethernet 1/0/4
vesr124-2-3(config-if-gi)# ip firewall disable
vesr124-2-3(config-if-gi)# ip address 10.10.30.1/24
vesr124-2-3(config-if-gi)# exit
vesr124-2-3(config)# do commit
Nothing to commit in configuration
2025-06-27T15:25:55+00:00 %CLI-I-CRIT: user admin from console
input: do commit
vesr124-2-3(config)# doconfirm
Nothing to confirm in configuration. You must commit some changes
first.
2025-06-27T15:26:01+00:00 %CLI-I-CRIT: user admin from console
input: do confirm
```

На маршрутизаторе vesr124-2-4 конфиг логически и структурно повторяет конфигурацию маршрутизатора vesr124-2-2. На этом маршрутизаторе конфигурация создаётся полностью новая по логике и структуре аналогичная той , что сделана для маршрутизатора vesr124-2-2. Изменяются адреса интерфейсов, имя туннеля и блок сети пула DHCP.

Можно либо повторить методику настройки туннеля, описанную в главе 8
либо перенести конфиг с маршрутизатора vesr124-2-2 можно так:

- Открыть консоли маршрутизаторов vesr124-2-2 , vesr124-2-4 нажав правую кнопку мыши на иконке маршрутизатора.
- Перейти в консоль маршрутизатора vesr124-2-2.
- В консоли маршрутизатора дать команду sh run.
- Скопировать весь конфиг выделением курсором мыши и нажав комбинацию клавиш ctrl+c.
- Перейти в консоль маршрутизатора vesr124-2-4 и дать config.
- Скопировать конфиг нажав комбинацию клавиш ctrl+v.

Затем предстоит поменять все локальные IP адреса интерфейсов и пулов.

Адрес интерфейсов должны быть такие:

```
vesr124-2-4(config)#  
vesr124-2-4(config)# interface gigabitethernet 1/0/1  
vesr124-2-4(config-if-gi)# description "WAN"  
vesr124-2-4(config-if-gi)# security-zone UNTRUST  
vesr124-2-4(config-if-gi)# ip address 10.10.30.2/24  
vesr124-2-4(config-if-gi)# exit  
vesr124-2-4(config)# interface gigabitethernet 1/0/2  
vesr124-2-4(config-if-gi)# description "LAN"  
vesr124-2-4(config-if-gi)# security-zone TRUST  
vesr124-2-4(config-if-gi)# ip address 172.16.3.1/24  
vesr124-2-4(config-if-gi)# exit  
vesr124-2-4(config)#
```

Адреса на туннеле и сам туннель такой:

```
vesr124-2-4(config)# tunnel gre 3
```

```
vesr124-2-4(config-gre)# mtu 1416
vesr124-2-4(config-gre)# security-zone UNTRUST
vesr124-2-4(config-gre)# local interface gigabitethernet 1/0/1
vesr124-2-4(config-gre)# remote address 10.10.10.2
vesr124-2-4(config-gre)# ip address 192.168.200.2/24
vesr124-2-4(config-gre)# enable
vesr124-2-4(config-gre)# exit
```

Изменяются описания объектных групп:

```
vesr124-2-4(config)# object-group network LAN_NETWORK
vesr124-2-4(config-object-group-network)# ip address-range
172.16.3.1-172.16.3
.254
vesr124-2-4(config-object-group-network)# exit
vesr124-2-4(config)# object-group network LAN_GW
vesr124-2-4(config-object-group-network)# ip address-range 172.16.3.1
vesr124-2-4(config-object-group-network)# exit
vesr124-2-4(config)# object-group network WANМеняется адрес
vesr124-2-4(config-object-group-network)# ip address-range 10.10.30.2
vesr124-2-4(config-object-group-network)# exit
vesr124-2-4(config)#
```

Меняется IP адреса в описании роута для шифрования:

```
vesr124-2-4(config)# security ike gateway ike_gw1
vesr124-2-4(config-ike-gw)# ike-policy ike_pol1
vesr124-2-4(config-ike-gw)# local address 10.10.30.2
vesr124-2-4(config-ike-gw)# local network 10.10.30.2/32 protocol gre
vesr124-2-4(config-ike-gw)# remote address 10.10.10.2
vesr124-2-4(config-ike-gw)# remote network 10.10.10.2/32 protocol gre
vesr124-2-4(config-ike-gw)# mode policy-based
vesr124-2-4(config-ike-gw)# exit
vesr124-2-4(config)#
```

Настраивается NAT SOURCE так:

```
vesr124-2-4(config)# nat source
vesr124-2-4(config-snat)# pool WAN
```

```

vesr124-2-4(config-snat-pool)# ip address-range 10.10.30.2
vesr124-2-4(config-snat-pool)# exit
vesr124-2-4(config-snat)# ruleset SNAT
vesr124-2-4(config-snat-ruleset)# to zone UNTRUST
vesr124-2-4(config-snat-ruleset)# rule 1
vesr124-2-4(config-snat-rule)# match source-address object-group
LAN_NETWORK
vesr124-2-4(config-snat-rule)# action source-nat interface

vesr124-2-4(config-snat-rule)# enable
vesr124-2-4(config-snat-rule)# exit
vesr124-2-4(config-snat-ruleset)# exit
vesr124-2-4(config-snat)# exit
vesr124-2-4(config)#

```

Редактируем блок маршрутизации:

```

ip route 0.0.0.0/0 10.10.30.1
ip route 10.10.10.0/24 10.10.10.1
ip route 10.10.20.0/24 10.10.20.1
ip route 172.16.1.0/24 tunnel gre 3
ip route 172.16.3.0/24 interface gigabitethernet 1/0/2

```

И в конце меняем настройки сервера dhcp:

```

ip dhcp-server pool LAN_NETWORK
network 172.16.3.0/24
default-lease-time 003:00:00
address-range 172.16.3.1-172.16.3.254
excluded-address-range 172.16.3.1,172.16.3.254
default-router 172.16.3.1
dns-server 77.88.8.8
exit
do commit

do confirm

```

Проверяем туннель и связность локальных сетей:

```

vesr124-2-4# sh ip int | i gre

```

static	192.168.200.2/24 primary	gre 3	Up	Up
--------	-----------------------------	-------	----	----

Туннель gre 3 активирован.

```
vesr124-2-4# ping 192.168.200.1
PING 192.168.200.1 (192.168.200.1) 56 bytes of data:
!!!!
--- 192.168.200.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 1.167/2.511/3.611/0.906 ms
vesr124-2-4#
```

И вторая сторона его отвечает на пинги. Проверка конфигурации и счетчиков:

```
vesr124-2-4# sh tunnels configuration gre 3
State:                               Enabled
Description:                         --
Mode:                                ip
Bridge group:                        --
VRF:                                 --
Local interface:                     gigabitethernet 1/0/1
Remote address:                      10.10.10.2
Calculates checksums for outgoing GRE packets: No
Requires that all input GRE packets were checksum: No
key:                                  --
TTL:                                  Inherit
DSCP:                                 Inherit
MTU:                                  1416
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:                --
vesr124-2-4# sh tunnels counters
```

Tunnel	Packets recv	Bytes recv	Errors recv	MC recv
gre 3	4816	406141	0	0

Tunnel	Packets sent	Bytes sent	Errors sent
gre 3	4826	404994	0

vesr124-2-4#

Проверка статуса шифрования в туннеле:

```
vesr124-2-4# sh security ipsec vpn status
```

Name	Local host	Remote host	Initiator spi
------	------------	-------------	---------------

Responder spi	State
---------------	-------

ipsec1	10.10.30.2	10.10.10.2	0x4c448e4336b6a2e7
0xc422df8f3fb052d1	Established		

vesr124-2-4#

Следует иметь в виду, что без настройки IPSEC туннель gre 3 работать не будет, поскольку на маршрутизаторе vesr124-2-1 шифрование было уже включено когда настраивался туннель gre 10.

Проверяем работу туннеля с машины MicroCoreLinux64.-3:

- Проверка назначенного адреса по dhcp.

```
gns3@box:~$ ip add | grep eth0: -A 2 | grep inet
inet 172.16.3.3/24 brd 172.16.3.255 scope global eth0
```

- Проверка связности локальных сетей командой ping.

```
gns3@box:~$ ping 172.16.1.2 -c 3
PING 172.16.1.2 (172.16.1.2): 56 data bytes
64 bytes from 172.16.1.2: seq=0 ttl=62 time=3.456 ms
64 bytes from 172.16.1.2: seq=1 ttl=62 time=4.837 ms
64 bytes from 172.16.1.2: seq=2 ttl=62 time=5.498 ms
```

--- 172.16.1.2 ping statistics ---

3 packets transmitted, 3 packets received, 0% packet loss

round-trip min/avg/max = 3.456/4.597/5.498 ms

Если использование браузера по какой то причине не подходит, то можно установить утилиту curl для чтения файлов с http сервера:

```
gns3@box:~$ tce-load -iw curl
curl.tcz.dep OK
libssh2.tcz.dep OK
libgcrypt.tcz.dep OK
Downloading: openssl.tcz
Connecting to repo.tinycorelinux.net (128.127.66.77:80)
openssl.tcz      100% |*****| 1116k
0:00:00 ETA
openssl.tcz: OK
Downloading: libgpg-error.tcz
Connecting to repo.tinycorelinux.net (128.127.66.77:80)
libgpg-error.tcz 100% |*****| 20480
0:00:00 ETA
libgpg-error.tcz: OK
Downloading: libgcrypt.tcz
Connecting to repo.tinycorelinux.net (128.127.66.77:80)
libgcrypt.tcz    100% |*****| 392k
0:00:00 ETA
libgcrypt.tcz: OK
Downloading: libssh2.tcz
Connecting to repo.tinycorelinux.net (128.127.66.77:80)
libssh2.tcz      100% |*****| 90112
0:00:00 ETA
libssh2.tcz: OK
Downloading: libidn.tcz
Connecting to repo.tinycorelinux.net (128.127.66.77:80)
libidn.tcz       100% |*****| 77824
0:00:00 ETA
libidn.tcz: OK
Downloading: curl.tcz
Connecting to repo.tinycorelinux.net (128.127.66.77:80)
curl.tcz         100% |*****| 272k
0:00:00 ETA
```

curl.tcz: OK

Проверка работы httpd сервера на маршрутизаторе vesr124-2-1
утилитой curl из командной строки машины MicroCoreLinux6.4-3:

```
gns3@box:~$ curl 172.16.1.2
<!doctype html>
<html lang="ru-RU">
<html>
  <head>
    <meta charset="utf-8"
    <title>Нью-Васюки->Арбатов</title>
  </head>
  <body>
    <br> Ударим автопробегом по бездорожью, разгильдяйству и
пофигизму!
  </body>
</html>
gns3@box:~$
```

И итоговая проверка из графического браузера firefox к чему мы так
долго шли:

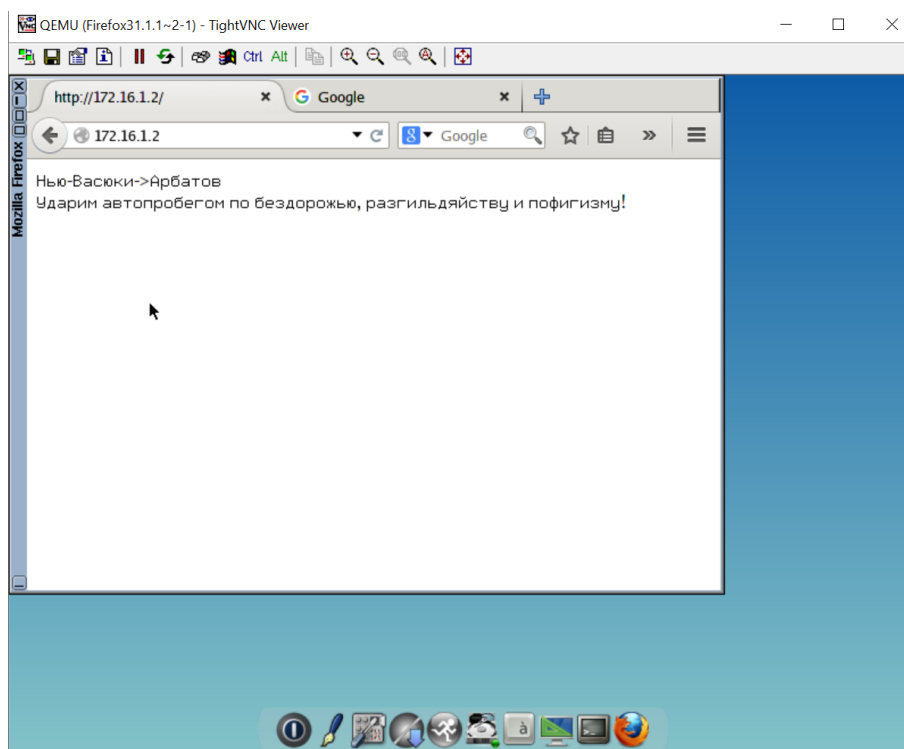


РИСУНОК 9-13. ДЕМОНСТРАЦИЯ РАБОТЫ СЕРВЕРА HTTPD .

ВЫВОДЫ ПО ГЛАВЕ

- Описана методика и приемы создания схемы подключения нового филиала с маршрутизатором vesr.
- Настроен маршрутизатор с сервисами NAT SOURCE, DHCP, static routing.
- Создан туннель по технологии пку+ipsec на двух маршрутизаторах.
- Установлены служебные утилиты.
- Настроен сервер busybox-httpd.
- Описаны команды настройки и проверки туннеля gre+ipsec.

В следующей главе будет описан порядок настройки протокола динамической маршрутизации OSPF применительно к изученной схеме подключения центрального офиса и двух его филиалов.

Глава 10. Настройка динамической (OSPF) маршрутизации в виртуальном маршрутизаторе vESR.

Цель этой работы:

В предыдущей главе было показано как строится сеть из трех территориально удаленных узлов в сети интернет- центрального офиса и двух филиалов. Настройка маршрутов для прохождения IP пакетов от узла к узлу описана командами статической маршрутизации. И при изменении параметров сети, придётся на каждом маршрутизаторе заново прописывать эти команды. В случае большого количества таких узлов это станет обременительным занятием и может привести к ошибкам в маршрутах. Что бы избежать такого применяются протоколы динамической маршрутизации, например, OSPF.

OSPF (Open Shortest Path First) — это протокол внутренней маршрутизации, который позволяет маршрутизаторам обмениваться маршрутной информацией внутри одной автономной системы.

Основная задача OSPF — определение оптимального пути для передачи данных между узлами сети на основе различных метрик (например, стоимости маршрута).

Некоторые особенности OSPF:

Динамическая маршрутизация. В отличие от статической маршрутизации, где маршруты прописываются вручную, OSPF автоматически адаптируется к изменениям в топологии сети.

Поддержка больших и сложных сетей. OSPF поддерживает разделение сети на области, что помогает улучшить масштабируемость и управляемость сети.

Отправка обновлений только при изменениях топологии. Это снижает нагрузку на сеть и экономит ресурсы.

Настроим динамическую маршрутизацию на примере схемы из предыдущей главы и уберём статику.

- Удаляем на каждом узловом маршрутизаторе (кроме vesr124-2-3) статические маршруты не локальные сети филиалов. На маршрутизаторе vesr124-2-1 смотрим доступность локальных сетей филиалов и какие маршруты идут в тоннели:

```
vesr124-2-1# ping 172.16.2.2
PING 172.16.2.2 (172.16.2.2) 56 bytes of data.
!!!!
--- 172.16.2.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4009ms
```

```

rtt min/avg/max/mdev = 2.242/5.848/13.450/4.069 ms
vesr124-2-1# ping 172.16.3.2
PING 172.16.3.2 (172.16.3.2) 56 bytes of data.
.!!!!
--- 172.16.3.2 ping statistics ---
5 packets transmitted, 4 received, 20% packet loss, time 4010ms
rtt min/avg/max/mdev = 4.207/6.374/8.481/1.970 ms

vesr124-2-1# sh run routing | i tunnel
ip route 172.16.2.0/24 tunnel gre 10
ip route 172.16.3.0/24 tunnel gre 3

```

- Удаляем эти маршруты из таблицы маршрутизатора:

```

vesr124-2-1(config)# no ip route 172.16.2.0/24
vesr124-2-1(config)# no ip route 172.16.3.0/24
vesr124-2-1(config)# do sh running-config routing | i tunnel
ip route 172.16.2.0/24 tunnel gre 10
ip route 172.16.3.0/24 tunnel gre 3
vesr124-2-1(config)# do commit
Configuration has been successfully applied and saved to flash. Commit
timer started, changes will be reverted in 600 seconds.
2025-06-30T12:56:50+00:00 %CLI-I-CRIT: user admin from console
input: do commit
vesr124-2-1(config)# do confirm
Configuration has been confirmed. Commit timer canceled.
2025-06-30T12:56:55+00:00 %CLI-I-CRIT: user admin from console
input: do confirm
vesr124-2-1(config)# exit
vesr124-2-1#

```

- Проверяем доступность сетей филиалов:

```

vesr124-2-1# ping 172.16.2.2
PING 172.16.2.2 (172.16.2.2) 56 bytes of data.
.....
--- 172.16.2.2 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4018ms

vesr124-2-1# ping 172.16.3.2
PING 172.16.3.2 (172.16.3.2) 56 bytes of data.
.....

```

```
--- 172.16.3.2 ping statistics ---  
5 packets transmitted, 0 received, 100% packet loss, time 4008ms  
vesr124-2-1#
```

Теперь маршрутов нет и сети не доступны. Настроим динамическую маршрутизацию для связи локальных сетей через туннельный интерфейс этого маршрутизатора vesr124-2-1:

- Создадим OSPF-процесс с идентификатором 1 и перейдём в режим конфигурирования протокола OSPF и создадим и включим требуемую область, включим OSPF-процесс:

```
vesr124-2-1#  
vesr124-2-1# config  
vesr124-2-1(config)# router ospf 1  
vesr124-2-1(config-ospf)# area 0.0.0.0  
vesr124-2-1(config-ospf-area)# enable  
vesr124-2-1(config-ospf-area)# exit  
vesr124-2-1(config-ospf)# enable  
vesr124-2-1(config-ospf)# exit  
vesr124-2-1(config)#
```

- Для установления соседства с другими маршрутизаторами привяжем их к OSPF-процессу и области.
- Далее включим на интерфейсе маршрутизацию по протоколу OSPF:

интерфейс gre 10 - для установления соседства с первым филиалом
интерфейс gre 3 - для установления соседства со вторым филиалом
интерфейс gi1/0/2 - для объявления локальных сетей

```
vesr124-2-1(config)# interface gigabitethernet 1/0/2  
vesr124-2-1(config-if-gi)# ip ospf instance 1  
vesr124-2-1(config-if-gi)# ip ospf  
vesr124-2-1(config-if-gi)# exit  
vesr124-2-1(config)# tunnel gre 10  
vesr124-2-1(config-gre)# ip ospf instance 1  
vesr124-2-1(config-gre)# ip ospf  
vesr124-2-1(config-gre)# exit  
vesr124-2-1(config)# tunnel gre 3  
vesr124-2-1(config-gre)# ip ospf instance 1
```

```
vesr124-2-1(config-gre)# ip ospf
vesr124-2-1(config-gre)# exit
vesr124-2-1(config)#
```

- Разрешаем трафик OSPF:

```
vesr124-2-1(config)#
vesr124-2-1(config)# security zone-pair UNTRUST self
vesr124-2-1(config-security-zone-pair)# rule 9
vesr124-2-1(config-security-zone-pair-rule)# description "OSPF"
vesr124-2-1(config-security-zone-pair-rule)# action permit
vesr124-2-1(config-security-zone-pair-rule)# match protocol ospf
vesr124-2-1(config-security-zone-pair-rule)# enable
vesr124-2-1(config-security-zone-pair-rule)# exit
vesr124-2-1(config-security-zone-pair)# exit
vesr124-2-1(config)# exit
Warning: you have uncommitted configuration changes.
vesr124-2-1#
```

- Применяем и переходим ко второму маршрутизатору vesr124-2-2:

```
vesr124-2-2# config
vesr124-2-2(config)# router ospf 1
vesr124-2-2(config-ospf)# area 0.0.0.0
vesr124-2-2(config-ospf-area)# enable
vesr124-2-2(config-ospf-area)# exit
vesr124-2-2(config-ospf)# enable
vesr124-2-2(config-ospf)# exit
vesr124-2-2(config)# interface gigabitethernet 1/0/2
vesr124-2-2(config-if-gi)# ip ospf instance 1
vesr124-2-2(config-if-gi)# ip ospf
vesr124-2-2(config-if-gi)# exit
vesr124-2-2(config)# tunnel gre 10
vesr124-2-2(config-gre)# ip ospf instance 1
vesr124-2-2(config-gre)# ip ospf
vesr124-2-2(config-gre)# enable
vesr124-2-2(config-gre)# exit
vesr124-2-2(config)#
```

- Применяем изменения в конфигурации и проверяем маршрутизацию и связность сетей:

```
vesr124-2-2(config)# do commit
Configuration has been successfully applied and saved to flash. Commit
timer started, changes will be reverted in 600 seconds.
2025-06-30T13:33:11+00:00 %CLI-I-CRIT: user admin from console
input: do commit
vesr124-2-2(config)# do confirm
Configuration has been confirmed. Commit timer canceled.
2025-06-30T13:33:14+00:00 %CLI-I-CRIT: user admin from console
input: do confirm
vesr124-2-2(config)# exit
```

- Смотрим на маршрутизаторе vesr124-2-1 и проверяем установление соседства:

```
vesr124-2-1# sh ip ospf neighbors
```

Router ID	Pri	State	DTime	Interface	Router IP
10.10.20.2	128	Full/BDR	00:35	gre 10	192.168.100.2

```
vesr124-2-1#
```

Рамкой красного цвета выделена связь обмена маршрутами OSPF через туннель gre 10.

- Проверяем таблицу маршрутизации:

```
vesr124-2-1# sh ip route
Codes: C - connected, S - static, R - RIP derived,
       O - OSPF derived, IA - OSPF inter area route,
       E1 - OSPF external type 1 route, E2 - OSPF external type 2 route
       B - BGP derived, D - DHCP derived, K - kernel route, V - VRRP
route
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       H - NHRP, * - FIB route
```

S	* 0.0.0.0/0	[1/0]	via 10.10.10.1 on gi1/0/1	[static
12:46:39]				
C	* 192.168.200.0/24	[0/0]	dev gre 3	[direct
12:46:39]				

```

C    * 192.168.100.0/24 [0/0]          dev gre 10          [direct
12:46:39]
C    * 172.16.1.0/24   [0/0]          dev gi1/0/2        [direct
12:46:39]
O    * 172.16.2.0/24   [150/1001]     via 192.168.100.2 on gre 10
[ospf1 13:33:24 from 10.10.20.2] (10.10.20.2)
C    * 10.10.10.0/24   [0/0]          dev gi1/0/1        [direct
12:46:39]
vesr124-2-1#

```

Рамкой красного цвета выделена маршрутизация по OSPF через туннель gre 10.

- Смотрим на маршрутизаторе vesr124-2-2 и проверяем установление соседства:

```

vesr124-2-2# sh ip ospf neighbors
Router ID    Pri State      DTime Interface      Router IP
-----
10.10.10.2   128 Full/DR    00:35 gre 10          192.168.100.1
vesr124-2-2#

```

Рамкой красного цвета выделена связь обмена маршрутами OSPF через туннель gre 10.

- Проверяем таблицу маршрутизации:

```

vesr124-2-2# sh ip route
Codes: C - connected, S - static, R - RIP derived,
O - OSPF derived, IA - OSPF inter area route,
E1 - OSPF external type 1 route, E2 - OSPF external type 2 route
B - BGP derived, D - DHCP derived, K - kernel route, V - VRRP
route
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
H - NHRP, * - FIB route

S    * 0.0.0.0/0       [1/0]          via 10.10.20.1 on gi1/0/1    [static
12:46:31]
C    * 10.10.20.0/24   [0/0]          dev gi1/0/1                [direct
12:46:31]

```

```
O * 192.168.200.0/24 [150/2000] via 192.168.100.1 on gre 10
[ospf1 13:33:24 from 10.10.10.2] (10.10.10.2)
```

```
C * 192.168.100.0/24 [0/0] dev gre 10 [direct
12:46:31]
```

```
S * 172.16.1.0/24 [1/0] dev gre 10 [static
12:46:31]
```

```
C * 172.16.2.0/24 [0/0] dev gi1/0/2 [direct
12:46:31]
```

Рамкой красного цвета выделена связь обмена маршрутами OSPF через туннель gre 10.

- Проверяем связность с клиентов
- Проверка первого филиала из центрального офиса:

MicroCoreLinux6.4-1 -> MicroCoreLinux6.4-2

```
gns3@box:~$ ip add | grep -A 3 eth0
5: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500
qdisc pfifo_fast state UP qlen 1000
    link/ether 0c:ec:ff:84:00:00 brd ff:ff:ff:ff:ff:ff
```

```
    inet 172.16.1.2/24 brd 172.16.1.255 scope global eth0
```

```
        valid_lft forever preferred_lft forever
    inet6 fe80::eec:ffff:fe84:0/64 scope link
        valid_lft forever preferred_lft forever
```

```
gns3@box:~$ ping 172.16.2.2 -c 3
```

```
PING 172.16.2.2 (172.16.2.2): 56 data bytes
64 bytes from 172.16.2.2: seq=0 ttl=62 time=4.293 ms
64 bytes from 172.16.2.2: seq=1 ttl=62 time=5.566 ms
64 bytes from 172.16.2.2: seq=2 ttl=62 time=7.609 ms
```

```
--- 172.16.2.2 ping statistics ---
```

```
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 4.293/5.822/7.609 ms
```

```
gns3@box:~$
```

- Трасса проходит чрез туннель gre 10:

```
gns3@box:~$ traceroute 172.16.2.2
```

```
traceroute to 172.16.2.2 (172.16.2.2), 30 hops max, 38 byte packets
```

```

1 172.16.1.1 (172.16.1.1) 0.007 ms 0.004 ms 0.767 ms
2 192.168.100.2 (192.168.100.2) 0.004 ms 1.942 ms 1.663 ms
3 172.16.2.2 (172.16.2.2) 2.932 ms 2.814 ms 0.003 ms
gns3@box:~$

```

- Проверка из первого филиала:
MicroCoreLinux6.4-2 -> MicroCoreLinux6.4-1

```

gns3@box:~$ ip add | grep -A 3 eth0
5: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500
qdisc pfifo_fast state UP qlen 1000
    link/ether 0c:5d:76:56:00:00 brd ff:ff:ff:ff:ff:ff
    inet 172.16.2.2/24 brd 172.16.2.255 scope global eth0
        valid_lft forever preferred_lft forever

```

```

gns3@box:~$ ping 172.16.1.2 -c 3

```

```

PING 172.16.1.2 (172.16.1.2): 56 data bytes
64 bytes from 172.16.1.2: seq=0 ttl=62 time=5.920 ms
64 bytes from 172.16.1.2: seq=1 ttl=62 time=6.993 ms
64 bytes from 172.16.1.2: seq=2 ttl=62 time=5.635 ms

```

```

--- 172.16.1.2 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 5.635/6.182/6.993 ms
gns3@box:~$

```

- Трасса проходит чрез туннель gre 10:

```

gns3@box:~$ traceroute 172.16.1.2
traceroute to 172.16.1.2 (172.16.1.2), 30 hops max, 38 byte packets
1 172.16.2.1 (172.16.2.1) 0.953 ms 0.003 ms 0.702 ms
2 192.168.100.1 (192.168.100.1) 1.756 ms 1.793 ms 1.573 ms
3 172.16.1.2 (172.16.1.2) 2.468 ms 2.599 ms 2.336 ms
gns3@box:~$

```

- переходим к маршрутизатору второго филиала vesr124-2-4:

настройки аналогичны тем , что были сделаны на маршрутизаторе первого филиала, за исключением названия туннеля.

```

vesr124-2-4#

```

```

vesr124-2-4# config
vesr124-2-4(config)# router ospf 1
vesr124-2-4(config-ospf)# area 0.0.0.0
vesr124-2-4(config-ospf-area)# enable
vesr124-2-4(config-ospf-area)# exit
vesr124-2-4(config-ospf)# enable
vesr124-2-4(config-ospf)# exit
vesr124-2-4(config)# int gigabitethernet 1/0/2
vesr124-2-4(config-if-gi)# ip ospf instance 1
vesr124-2-4(config-if-gi)# ip ospf
vesr124-2-4(config-if-gi)# exit
vesr124-2-4(config)# tunnel gre 3
vesr124-2-4(config-gre)# ip ospf instance 1
vesr124-2-4(config-gre)# ip ospf
vesr124-2-4(config-gre)# enable
vesr124-2-4(config-gre)# exit
vesr124-2-4(config)# security zone-pair UNTRUST self
vesr124-2-4(config-security-zone-pair)# rule 9
vesr124-2-4(config-security-zone-pair-rule)# description "OSPF"
vesr124-2-4(config-security-zone-pair-rule)# action permit
vesr124-2-4(config-security-zone-pair-rule)# match protocol ospf
vesr124-2-4(config-security-zone-pair-rule)# enable
vesr124-2-4(config-security-zone-pair-rule)# exit
vesr124-2-4(config-security-zone-pair)# exit
vesr124-2-4(config)# exit
Warning: you have uncommitted configuration changes.
vesr124-2-4# commit
Configuration has been successfully applied and saved to flash. Commit
timer started, changes will be reverted in 600 seconds.
2025-07-01T10:23:15+00:00 %CLI-I-CRIT: user admin from console
input: commit
vesr124-2-4# confirm
Configuration has been confirmed. Commit timer canceled.
2025-07-01T10:23:18+00:00 %CLI-I-CRIT: user admin from console
input: confirm
vesr124-2-4#

```

- Смотрим на маршрутизаторе vesr124-2-1 и проверяем установление соседства:

```

vesr124-2-1# sh ip ospf neighbors
Router ID    Pri State      DTime Interface      Router IP

```

```

-----  ---  -----  -----
10.10.30.2    128 Full/BDR    00:31 gre 3        192.168.200.2
10.10.20.2    128 Full/DR    00:38 gre 10       192.168.100.2
vesr124-2-1#

```

Появился второй сосед по обмену маршрутами-выделено красной рамкой.

- Проверяем таблицу маршрутизации:

```

vesr124-2-1# sh ip route
Codes: C - connected, S - static, R - RIP derived,
       O - OSPF derived, IA - OSPF inter area route,
       E1 - OSPF external type 1 route, E2 - OSPF external type 2 route
       B - BGP derived, D - DHCP derived, K - kernel route, V - VRRP
route
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       H - NHRP, * - FIB route

S    * 0.0.0.0/0      [1/0]        via 10.10.10.1 on gi1/0/1      [static
09:58:04]
C    * 192.168.200.0/24 [0/0]          dev gre 3                    [direct
09:58:05]
C    * 192.168.100.0/24 [0/0]          dev gre 10                   [direct
09:58:05]
O    * 172.16.3.0/24   [150/1001]   via 192.168.200.2 on gre 3
[ospf1 10:23:19 from 10.10.30.2] (10.10.30.2)
C    * 172.16.1.0/24   [0/0]          dev gi1/0/2                  [direct
09:58:05]
O    * 172.16.2.0/24   [150/1001]   via 192.168.100.2 on gre 10
[ospf1 09:58:55 from 10.10.20.2] (10.10.20.2)
C    * 10.10.10.0/24   [0/0]          dev gi1/0/1                  [direct
09:58:05]
vesr124-2-1#

```

Появился второй маршрут-выделено красной рамкой.

Переходим на маршрутизатор второго филиала и проверяем там:

- Смотрим на маршрутизаторе vesr124-2-4 и проверяем установление соседства:

```
vesr124-2-4# sh ip ospf neighbors
```

Router ID	Pri	State	DTime	Interface	Router IP
10.10.10.2	128	Full/DR	00:34	gre 3	192.168.200.1

Router ID	Pri	State	DTime	Interface	Router IP
10.10.10.2	128	Full/DR	00:34	gre 3	192.168.200.1

Router ID	Pri	State	DTime	Interface	Router IP
10.10.10.2	128	Full/DR	00:34	gre 3	192.168.200.1

```
vesr124-2-4#
```

Появился сосед по обмену на втором маршруторе-выделено красной рамкой.

- Проверяем таблицу маршрутизации:

```
vesr124-2-4# sh ip route
```

Codes: C - connected, S - static, R - RIP derived,

O - OSPF derived, IA - OSPF inter area route,

E1 - OSPF external type 1 route, E2 - OSPF external type 2 route

B - BGP derived, D - DHCP derived, K - kernel route, V - VRRP

route

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

H - NHRP, * - FIB route

```
S * 0.0.0.0/0 [1/0] via 10.10.30.1 on gi1/0/1 [static
09:58:15]
```

```
C * 192.168.200.0/24 [0/0] dev gre 3 [direct
09:58:15]
```

```
O * 192.168.100.0/24 [150/2000] via 192.168.200.1 on gre 3
[ospf1 10:23:21 from 10.10.20.2] (10.10.20.2)
```

```
C * 172.16.3.0/24 [0/0] dev gi1/0/2 [direct
09:58:15]
```

```
S * 172.16.1.0/24 [1/0] dev gre 3 [static
09:58:15]
```

```
O * 172.16.2.0/24 [150/2001] via 192.168.200.1 on gre 3
[ospf1 10:23:21 from 10.10.20.2] (10.10.20.2)
```

```
C * 10.10.30.0/24 [0/0] dev gi1/0/1 [direct
09:58:15]
```

```
vesr124-2-4#
```

Динамический маршрут появился-выделен красной рамкой.

- Проверяем связность с клиентов

- Проверка второго филиала из центрального офиса:

MicroCoreLinux6.4-1 -> MicroCoreLinux6.4-3

```
gns3@box:~$ ip add | grep -A 3 eth0
5: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500
qdisc pfifo_fast state UP qlen 1000
    link/ether 0c:ec:ff:84:00:00 brd ff:ff:ff:ff:ff:ff
    inet 172.16.1.2/24 brd 172.16.1.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::eec:ffff:fe84:0/64 scope link
        valid_lft forever preferred_lft forever
gns3@box:~$ ping 172.16.3.2 -c 3
PING 172.16.3.2 (172.16.3.2): 56 data bytes
64 bytes from 172.16.3.2: seq=0 ttl=62 time=4.294 ms
64 bytes from 172.16.3.2: seq=1 ttl=62 time=6.647 ms
64 bytes from 172.16.3.2: seq=2 ttl=62 time=5.617 ms

--- 172.16.3.2 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 4.294/5.519/6.647 ms
gns3@box:~$
```

- Трасса проходит через туннель gre 3:

```
gns3@box:~$ traceroute 172.16.3.2
traceroute to 172.16.3.2 (172.16.3.2), 30 hops max, 38 byte packets
 1 172.16.1.1 (172.16.1.1) 1.027 ms 0.844 ms 0.309 ms
 2 192.168.200.2 (192.168.200.2) 2.981 ms 1.647 ms 2.462 ms
 3 172.16.3.2 (172.16.3.2) 2.597 ms 2.787 ms 2.321 ms
gns3@box:~$
```

- Проверка из второго филиала:

MicroCoreLinux6.4-3 -> MicroCoreLinux6.4-1

```
gns3@box:~$ ip add | grep -A 3 eth0 ; ping 172.16.1.2 -c 3
5: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500
qdisc pfifo_fast state UP qlen 1000
    link/ether 0c:e5:41:79:00:00 brd ff:ff:ff:ff:ff:ff
```

```
inet 172.16.3.3/24 brd 172.16.3.255 scope global eth0
```

```
valid_lft forever preferred_lft forever
```

```
PING 172.16.1.2 (172.16.1.2): 56 data bytes
```

```
64 bytes from 172.16.1.2: seq=0 ttl=62 time=4.707 ms
```

```
64 bytes from 172.16.1.2: seq=1 ttl=62 time=6.203 ms
```

```
64 bytes from 172.16.1.2: seq=2 ttl=62 time=5.530 ms
```

```
--- 172.16.1.2 ping statistics ---
```

```
3 packets transmitted, 3 packets received, 0% packet loss
```

```
round-trip min/avg/max = 4.707/5.480/6.203 ms
```

```
gns3@box:~$
```

- Трасса проходит чрез туннель gre 3:

```
gns3@box:~$ traceroute 172.16.1.2
```

```
traceroute to 172.16.1.2 (172.16.1.2), 30 hops max, 38 byte packets
```

```
1 172.16.3.1 (172.16.3.1) 0.007 ms 1.007 ms 0.821 ms
```

```
2 192.168.200.1 (192.168.200.1) 2.131 ms 0.004 ms 0.273 ms
```

```
3 172.16.1.2 (172.16.1.2) 1.299 ms 0.263 ms 2.470 ms
```

```
gns3@box:~$
```

- Проверка доступности сервисов sshd и httpd на сети центрального офиса:

```
gns3@box:~$ ssh gns3@172.16.1.2
```

```
-sh: ssh: not found
```

Нет машине утилиты-обновляем пакеты и ставим:

```
gns3@box:~$ tce-update
```

```
Checking for Easy Mode Operation... OK
```

```
Press Enter key to begin batch update of extensions in /sda1/tce  
or enter any char to exit now:
```

```
Checking Tiny Core Applications in /mnt/sda1/tce/optional
```

```
Your system is up-to-date.
```

```
Press Enter key.
```

```
gns3@box:~$ tce-load -iw openssh
```

```
openssh.tcz.dep OK
```

```
Downloading: openssh.tcz
```

```
Connecting to repo.tinycorelinux.net (128.127.66.77:80)
```

```
openssh.tcz      100% |*****| 1992k
0:00:00 ETA
```

```
openssh.tcz: OK
```

```
gns3@box:~$ ssh gns3@172.16.1.2
```

```
The authenticity of host '172.16.1.2 (172.16.1.2)' can't be established.
```

```
ECDSA key fingerprint is
```

```
29:52:34:28:a8:c7:f3:49:f1:ac:fb:5c:b3:99:25:0c.
```

```
Are you sure you want to continue connecting (yes/no)? yes
```

```
Warning: Permanently added '172.16.1.2' (ECDSA) to the list of known
hosts.
```

```
gns3@172.16.1.2's password:gns3
```

```
( '>')
```

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

```
(/_--_-\)      www.tinycorelinux.net
```

```
gns3@box:~$ exit
```

Connection to 172.16.1.2 closed. – сервис sshd на машине в
центральной офисе работает.

```
gns3@box:~$ curl 172.16.1.2
```

```
curl: (7) Failed to connect to 172.16.1.2 port 80: Connection refused
```

Проверяем есть сервис httpd на машине MicroCoreLinux6.4-1 в сети
центрального офиса:

```
gns3@box:~$ netstat -tuln | grep 80
```

```
gns3@box:~$
```

Пусто. Не запущен сервис httpd на машине в центральной офисе—
нужно его запустить:

```
gns3@box:~$ sudo /usr/local/httpd/sbin/httpd -p 80 -h /home/gns3/
```

```
gns3@box:~$ netstat -tuln | grep 80
```

```
tcp      0      0 0.0.0.0:80          0.0.0.0:*          LISTEN
```

Снова переходим на машину MicroCoreLinux6.4-3 в сети второго
филиала. Проверяем вначале утилитой curl (она была установлена в
предыдущей главе):

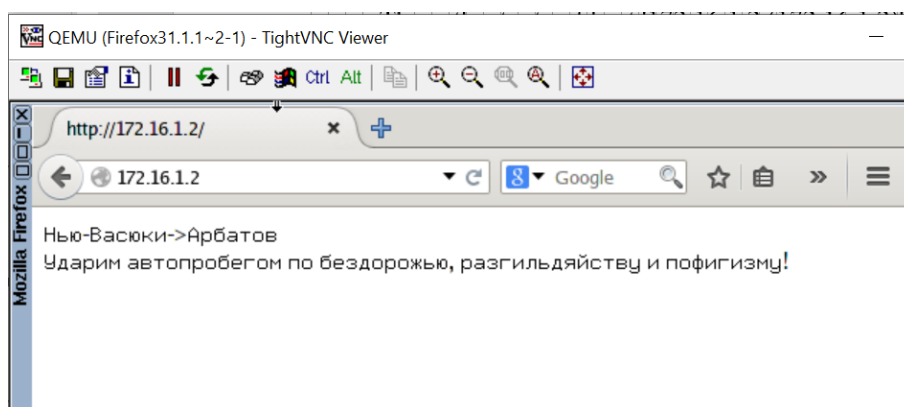
```
gns3@box:~$
```

```
gns3@box:~$ curl 172.16.1.2
```

```
<!doctype html>
```

```
<html lang="ru-RU">
```

```
<html>
<head>
  <meta charset="utf-8"
  <title>Нью-Васюки->Арбатов</title>
</head>
<body>
  <br> Ударим автопробегом по бездорожью, разгильдяйству и
пофигизму!
</body>
</html>
gns3@box:~$
```



**РИСУНОК 10-1. ЭКРАН ПРОВЕРКИ РАБОТЫ СЕРВИСА БРАУЗЕРОМ
FIREFOX.**

Проверено, всё работает.

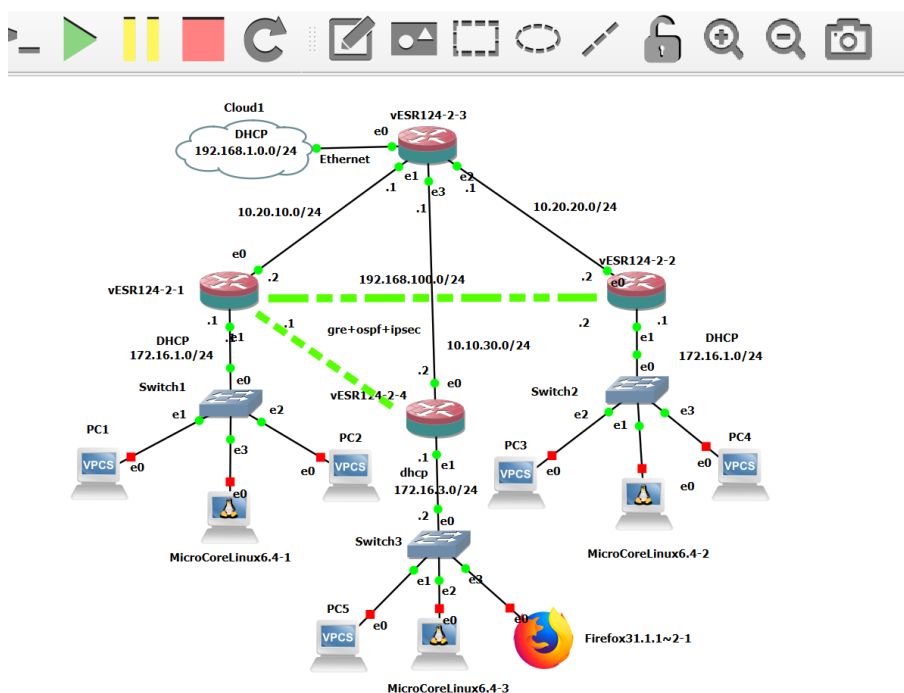


Рисунок 10-2. ИТОГОВАЯ СХЕМА ПО ГЛАВЕ 10.

Конфигурация устройств.

Конфигурация маршрутизатора в центральном офисе vesr124-2-1:
hostname vesr124-2-1

```
object-group service dhcp_service
  port-range 67
exit
object-group service dhcp_client
  port-range 68
exit
object-group service ssh
  port-range 22
exit
object-group service SSH
  port-range 2222
exit
object-group service TRACEROUTE
  port-range 33434-33534
exit
```

```
object-group network WAN
  ip address-range 10.10.10.2
```

```
exit
object-group network clients
  ip address-range 192.168.10.0-192.168.10.254
  ip address-range 192.168.151.1-192.168.151.254
  ip address-range 10.10.10.1-10.10.10.254
  ip address-range 10.10.20.1-10.10.20.254
  ip address-range 172.16.2.1-172.16.2.254
exit
object-group network SERVER_IP
  ip address-range 172.16.1.2
exit
object-group network LAN_NETWORK
  ip address-range 172.16.1.1-172.16.1.254
exit
object-group network LAN_GW
  ip address-range 172.16.1.1
exit

syslog max-files 3
syslog file-size 512
syslog file tmpsys:syslog/default
  severity info
exit
syslog console
  virtual-terminal
exit

username admin
  password encrypted
$6$Kx1jB3DT6zH05CQ7$WqbKGSvl/35jvx.NKDc6R5NpD5uy2623zfbWAO
TPhNOQgnR.zXxQzlgYwESdbxOWSyhPPNojy0Q0.pMvR6Ld/
exit
username rinat
  password encrypted
$6$T37FYJy.i38S36O0$vHt9c.g0yzphZ5PJNwkmOvJJ36dSvMbr7qRSJnDWh
prk4f8OI5d1oNdT6jmqUsXMbfgRFDd4RK3Ugeu0jLZ9w/
  privilege 15
exit

domain lookup enable

security zone UNTRUST
```

```
exit
security zone TRUST
exit
```

```
router ospf 1
  area 0.0.0.0
  enable
exit
enable
exit
```

```
interface gigabitethernet 1/0/1
  description "WAN"
  security-zone UNTRUST
  ip address 10.10.10.2/24
exit
```

```
interface gigabitethernet 1/0/2
  description "LAN_NET"
  security-zone TRUST
  ip address 172.16.1.1/24
  ip ospf instance 1
  ip ospf
exit
```

```
interface gigabitethernet 1/0/3
  shutdown
  ip address dhcp
exit
```

```
tunnel gre 3
  ttl 18
  mtu 1416
  security-zone UNTRUST
  local address 10.10.10.2
  remote address 10.10.30.2
  ip address 192.168.200.1/24
  ip ospf instance 1
  ip ospf
  enable
exit
tunnel gre 10
  ttl 18
  security-zone UNTRUST
```

```
local address 10.10.10.2
remote address 10.10.20.2
ip address 192.168.100.1/24
ip ospf instance 1
ip ospf
enable
exit

security zone-pair TRUST self
rule 1
  description "ICMP"
  action permit
  match protocol icmp
  enable
exit
rule 2
  action permit
  match protocol udp
  enable
exit
rule 3
  description "GRE"
  action permit
  match protocol gre
  enable
exit
rule 4
  action permit
  match protocol udp
  match source-port object-group dhcp_client
  match destination-port object-group dhcp_service
  enable
exit
rule 10
  action permit
  match protocol tcp
  enable
exit
exit
security zone-pair TRUST UNTRUST
rule 1
  action permit
```

```
    match protocol icmp
    enable
exit
rule 2
    action permit
    match protocol udp
    enable
exit
rule 3
    description "GRE"
    action permit
    match protocol gre
    enable
exit
rule 10
    action permit
    match protocol tcp
    enable
exit
exit
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
rule 3
    description "TRACEROUTE"
    action permit
    match protocol udp
    enable
exit
rule 4
    description "ESP"
    action permit
```

```
    match protocol esp
    enable
exit
rule 5
    description "AH"
    action permit
    match protocol ah
    enable
exit
rule 9
    description "OSPF"
    action permit
    match protocol ospf
    enable
exit
rule 10
    action permit
    match protocol tcp
    match source-address object-group clients
    match destination-address object-group WAN
    match destination-port object-group ssh
    enable
exit
exit
security zone-pair UNTRUST TRUST
rule 1
    description "ICMP"
    action permit
    match protocol icmp
    enable
exit
rule 2
    description "GRE"
    action permit
    match protocol gre
    enable
exit
rule 3
    description "TRACEROUTE"
    action permit
    match protocol udp
    enable
```

```
exit
rule 10
  action permit
  match protocol tcp
  match destination-address object-group SERVER_IP
  enable
exit
exit

security ike proposal ike_prop1
  authentication algorithm md5
  encryption algorithm aes128
  dh-group 2
exit

security ike policy ike_pol1
  pre-shared-key ascii-text encrypted AC94107EA75F5AFF
  proposal ike_prop1
exit

security ike gateway ike_gw1
  ike-policy ike_pol1
  local address 10.10.10.2
  local network 10.10.10.2/32 protocol gre
  remote address 10.10.20.2
  remote network 10.10.20.2/32 protocol gre
  mode policy-based
exit
security ike gateway ike_gw2
  ike-policy ike_pol1
  local address 10.10.10.2
  local network 10.10.10.2/32 protocol gre
  remote address 10.10.30.2
  remote network 10.10.30.2/32 protocol gre
  mode policy-based
exit

security ipsec proposal ipsec_prop1
  authentication algorithm md5
  encryption algorithm aes128
  pfs dh-group 2
exit
```

```
security ipsec policy ipsec_pol1  
  proposal ipsec_prop1  
exit
```

```
security ipsec vpn ipsec1  
  ike establish-tunnel route  
  ike gateway ike_gw1  
  ike ipsec-policy ipsec_pol1  
  enable
```

```
exit
```

```
security ipsec vpn ipsec2  
  ike establish-tunnel route  
  ike gateway ike_gw2  
  ike ipsec-policy ipsec_pol1  
  enable
```

```
exit
```

```
security passwords default-expired
```

```
nat destination  
  pool SERVER_POOL  
  ip address 172.16.1.2  
  ip port 22  
exit  
ruleset DNAT  
  from zone UNTRUST  
  rule 10  
    match protocol tcp  
    match destination-port object-group SSH  
    action destination-nat pool SERVER_POOL  
    enable  
  exit  
exit  
exit
```

```
nat source  
  pool WAN  
  ip address-range 10.10.10.2  
exit  
ruleset SNAT  
  to zone UNTRUST
```

```
rule 1
  match source-address object-group LAN_NETWORK
  action source-nat interface
  enable
exit
exit
exit
```

```
ip dhcp-server
ip dhcp-server pool LAN_NETWORK
  network 172.16.1.0/24
  default-lease-time 003:00:00
  address-range 172.16.1.3-172.16.1.254
  address 172.16.1.2 mac-address 0c:ec:ff:84:00:00
  default-router 172.16.1.1
  dns-server 77.88.8.8
exit
```

```
ip route 0.0.0.0/0 10.10.10.1
ip route 10.10.20.0/24 10.10.20.1
ip route 10.10.30.0/24 10.10.30.1
ip route 172.16.1.0/24 interface gigabitethernet 1/0/2
```

```
ip ssh server
```

```
ntp enable
ntp broadcast-client enable
```

```
licence-manager
  host address elm.eltex-co.ru
exit
```

Конфигурация маршрутизатора в первом филиале vesr124-2-2:

```
hostname vesr124-2-2
```

```
object-group service dhcp_service
  port-range 67
exit
object-group service dhcp_client
  port-range 68
exit
```

```
object-group service TRACEROUTE
  port-range 33434-33534
exit
```

```
object-group network LAN_NETWORK
  ip address-range 172.16.2.1-172.16.2.254
exit
```

```
object-group network LAN_GW
  ip address-range 172.16.2.1
exit
```

```
object-group network WAN
  ip address-range 10.10.20.2
exit
```

```
object-group network clients
  ip address-range 192.168.10.0-192.168.10.254
  ip address-range 192.168.151.1-192.168.151.254
  ip address-range 10.10.10.1-10.10.10.254
  ip address-range 10.10.20.1-10.10.20.254
  ip address-range 172.16.1.0-172.16.2.254
exit
```

```
syslog max-files 3
syslog file-size 512
syslog file tmpsys:syslog/default
  severity info
exit
syslog console
  virtual-terminal
exit
```

```
username admin
  password encrypted
$6$IB0aLOlcTz4bCj3C$.wb4QEOgQALUdzELWRMrUsSm3qP31ijGHFq6p7
rtnZtaPiwTLb5Y2N7dt9fvK/aNIULZ1yEzK6CM5u0uMiNtn/
exit
```

```
domain lookup enable
```

```
security zone TRUST
exit
security zone UNTRUST
exit
```

```
router ospf 1
  area 0.0.0.0
  enable
exit
enable
exit

interface gigabitethernet 1/0/1
  description "WAN"
  security-zone UNTRUST
  ip address 10.10.20.2/24
exit
interface gigabitethernet 1/0/2
  description "LAN"
  security-zone TRUST
  ip address 172.16.2.1/24
  ip ospf instance 1
  ip ospf
exit

tunnel gre 10
  ttl 18
  security-zone UNTRUST
  local address 10.10.20.2
  remote address 10.10.10.2
  ip address 192.168.100.2/24
  ip ospf instance 1
  ip ospf
  enable
exit

security zone-pair TRUST self
  rule 1
    description "ICMP"
    action permit
    match protocol icmp
    enable
  exit
  rule 2
    description "GRE"
    action permit
```

```
    match protocol gre
    enable
exit
rule 3
    description "TRACEROUTE"
    action permit
    match protocol udp
    enable
exit
rule 4
    action permit
    match protocol udp
    match source-port object-group dhcp_client
    match destination-port object-group dhcp_service
    enable
exit
rule 10
    action permit
    match protocol tcp
    enable
exit
exit
security zone-pair TRUST UNTRUST
rule 1
    description "ICMP"
    action permit
    match protocol icmp
    enable
exit
rule 2
    description "GRE"
    action permit
    match protocol gre
    enable
exit
rule 3
    description "TRACEROUTE"
    action permit
    match protocol udp
    enable
exit
rule 10
```

```
        action permit
        match protocol tcp
        enable
    exit
exit
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
rule 3
    description "TRACEROUTE"
    action permit
    match protocol udp
    enable
exit
rule 4
    description "ESP"
    action permit
    match protocol esp
    enable
exit
rule 5
    description "AH"
    action permit
    match protocol ah
    enable
exit
rule 9
    description "OSPF"
    action permit
    match protocol ospf
    enable
exit
```

```
rule 10
  action permit
  match protocol tcp
  enable
exit
exit
security zone-pair UNTRUST TRUST
rule 1
  description "ICMP"
  action permit
  match protocol icmp
  enable
exit
rule 2
  description "GRE"
  action permit
  match protocol gre
  enable
exit
rule 3
  description "TRACEROUTE"
  action permit
  match protocol udp
  enable
exit
rule 10
  action permit
  match protocol tcp
  enable
exit
exit

security ike proposal ike_prop1
  authentication algorithm md5
  encryption algorithm aes128
  dh-group 2
exit

security ike policy ike_pol1
  pre-shared-key ascii-text encrypted AC94107EA75F5AFF
  proposal ike_prop1
exit
```

```
security ike gateway ike_gw1
  ike-policy ike_pol1
  local address 10.10.20.2
  local network 10.10.20.2/32 protocol gre
  remote address 10.10.10.2
  remote network 10.10.10.2/32 protocol gre
  mode policy-based
exit
```

```
security ipsec proposal ipsec_prop1
  authentication algorithm md5
  encryption algorithm aes128
  pfs dh-group 2
exit
```

```
security ipsec policy ipsec_pol1
  proposal ipsec_prop1
exit
```

```
security ipsec vpn ipsec1
  ike establish-tunnel route
  ike gateway ike_gw1
  ike ipsec-policy ipsec_pol1
  enable
exit
```

```
security passwords default-expired
```

```
nat source
  pool WAN
  ip address-range 10.10.10.2
  exit
ruleset SNAT
  to zone UNTRUST
  rule 1
    match source-address object-group LAN_NETWORK
    action source-nat interface
    enable
  exit
exit
exit
```

```
ip dhcp-server
ip dhcp-server pool LAN_NETWORK
  network 172.16.2.0/24
  default-lease-time 003:00:00
  address-range 172.16.2.1-172.16.2.254
  excluded-address-range 172.16.2.1,172.16.2.254
  default-router 172.16.2.1
  dns-server 77.88.8.8
exit

ip route 0.0.0.0/0 10.10.20.1
ip route 10.10.10.0/24 10.10.10.1
ip route 10.10.30.0/24 10.10.30.1
ip route 172.16.1.0/24 tunnel gre 10
ip route 172.16.2.0/24 interface gigabitethernet 1/0/2

ip ssh server

ntp enable
ntp broadcast-client enable

licence-manager
  host address elm.eltex-co.ru
exit

Конфигурация маршрутизатора во втором филиале vesr124-2-4:
hostname vesr124-2-4

object-group service dhcp_service
  port-range 67
exit
object-group service dhcp_client
  port-range 68
exit
object-group service TRACEROUTE
  port-range 33434-33534
exit

object-group network LAN_NETWORK
  ip address-range 172.16.3.1-172.16.3.254
exit
```

```
object-group network LAN_GW
  ip address-range 172.16.3.1
exit
object-group network WAN
  ip address-range 10.10.30.2
exit
object-group network clients
  ip address-range 192.168.10.0-192.168.10.254
  ip address-range 192.168.151.1-192.168.151.254
  ip address-range 10.10.10.1-10.10.10.254
  ip address-range 10.10.20.1-10.10.20.254
  ip address-range 172.16.1.0-172.16.2.254
exit

syslog max-files 3
syslog file-size 512
syslog file tmpsys:syslog/default
  severity info
exit
syslog console
  virtual-serial
exit

username admin
  password encrypted
$6$IB0aLOlcTz4bCj3C$.wb4QEOgQALUdzELWRMrUsSm3qP31ijGHFq6p7
rtnZtaPiwTLb5Y2N7dt9fvK/aNIULZ1yEzK6CM5u0uMiNtn/
exit

domain lookup enable

security zone TRUST
exit
security zone UNTRUST
exit

router ospf 1
  area 0.0.0.0
  enable
  exit
  enable
exit
```

```
interface gigabitethernet 1/0/1
  description "WAN"
  security-zone UNTRUST
  ip address 10.10.30.2/24
exit
```

```
interface gigabitethernet 1/0/2
  description "LAN"
  security-zone TRUST
  ip address 172.16.3.1/24
  ip ospf instance 1
  ip ospf
exit
```

```
tunnel gre 3
  mtu 1416
  security-zone UNTRUST
  local interface gigabitethernet 1/0/1
  remote address 10.10.10.2
  ip address 192.168.200.2/24
  ip ospf instance 1
  ip ospf
  enable
exit
```

```
security zone-pair TRUST self
  rule 1
    description "ICMP"
    action permit
    match protocol icmp
    enable
  exit
  rule 2
    description "GRE"
    action permit
    match protocol gre
    enable
  exit
  rule 3
    description "TRACEROUTE"
    action permit
    match protocol udp
```

```
    enable
  exit
rule 4
  action permit
  match protocol udp
  match source-port object-group dhcp_client
  match destination-port object-group dhcp_service
  enable
exit
rule 10
  action permit
  match protocol tcp
  enable
exit
exit
security zone-pair TRUST UNTRUST
rule 1
  description "ICMP"
  action permit
  match protocol icmp
  enable
exit
rule 2
  description "GRE"
  action permit
  match protocol gre
  enable
exit
rule 3
  description "TRACEROUTE"
  action permit
  match protocol udp
  enable
exit
rule 10
  action permit
  match protocol tcp
  enable
exit
exit
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
rule 3
description "TRACEROUTE"
action permit
match protocol udp
enable
exit
rule 4
description "ESP"
action permit
match protocol esp
enable
exit
rule 5
description "AH"
action permit
match protocol ah
enable
exit
rule 9
description "OSPF"
action permit
match protocol ospf
enable
exit
rule 10
action permit
match protocol tcp
enable
exit
exit
security zone-pair UNTRUST TRUST
```

```
rule 1
  description "ICMP"
  action permit
  match protocol icmp
  enable
exit
rule 2
  description "GRE"
  action permit
  match protocol gre
  enable
exit
rule 3
  description "TRACEROUTE"
  action permit
  match protocol udp
  enable
exit
rule 10
  action permit
  match protocol tcp
  enable
exit
exit

security ike proposal ike_prop1
  authentication algorithm md5
  encryption algorithm aes128
  dh-group 2
exit

security ike policy ike_pol1
  pre-shared-key ascii-text encrypted AC94107EA75F5AFF
  proposal ike_prop1
exit

security ike gateway ike_gw1
  ike-policy ike_pol1
  local address 10.10.30.2
  local network 10.10.30.2/32 protocol gre
  remote address 10.10.10.2
  remote network 10.10.10.2/32 protocol gre
```

```
mode policy-based
exit
```

```
security ipsec proposal ipsec_prop1
  authentication algorithm md5
  encryption algorithm aes128
  pfs dh-group 2
exit
```

```
security ipsec policy ipsec_pol1
  proposal ipsec_prop1
exit
```

```
security ipsec vpn ipsec1
  ike establish-tunnel route
  ike gateway ike_gw1
  ike ipsec-policy ipsec_pol1
  enable
exit
```

```
security passwords default-expired
```

```
nat source
  pool WAN
    ip address-range 10.10.30.2
  exit
  ruleset SNAT
    to zone UNTRUST
    rule 1
      match source-address object-group LAN_NETWORK
      action source-nat interface
      enable
    exit
  exit
exit
```

```
ip dhcp-server
ip dhcp-server pool LAN_NETWORK
  network 172.16.3.0/24
  default-lease-time 003:00:00
  address-range 172.16.3.1-172.16.3.254
  excluded-address-range 172.16.3.1,172.16.3.254
```

```
default-router 172.16.3.1
```

```
dns-server 77.88.8.8
```

```
exit
```

```
ip route 0.0.0.0/0 10.10.30.1
```

```
ip route 10.10.10.0/24 10.10.10.1
```

```
ip route 10.10.20.0/24 10.10.20.1
```

```
ip route 172.16.1.0/24 tunnel gre 3
```

```
ip route 172.16.3.0/24 interface gigabitethernet 1/0/2
```

```
ip ssh server
```

```
ntp enable
```

```
ntp broadcast-client enable
```

```
licence-manager
```

```
host address elm.eltex-co.ru
```

```
exit
```

Конфигурация маршрутизатора эмулирующего подключения сети к
провайдеру интернет vesr124-2-3:

```
hostname vesr124-2-3
```

```
syslog max-files 3
```

```
syslog file-size 512
```

```
syslog file tmpsys:syslog/default
```

```
severity info
```

```
exit
```

```
syslog console
```

```
virtual-terminal
```

```
exit
```

```
username admin
```

```
password encrypted
```

```
$6$QQYPCWq74yW353Id$XWrytd1iPLBLzB89IzSqLuhx5tQnmH3JvL8Pny0  
ykY8Kxx1gtbafWOLNRkHnDvoFGSrHkTgprXUA7a4ZYZeJx1
```

```
exit
```

```
domain lookup enable
```

```
domain name-server 77.88.8.8
```

```
interface gigabitethernet 1/0/1
  description "UPLINK_2_WORLD"
  ip firewall disable
  ip address dhcp
exit
interface gigabitethernet 1/0/2
  description "link2 vesr124-2-1"
  ip firewall disable
  ip address 10.10.10.1/24
exit
interface gigabitethernet 1/0/3
  description "Link2 vesr124-2-2"
  ip firewall disable
  ip address 10.10.20.1/24
exit
interface gigabitethernet 1/0/4
  ip firewall disable
  ip address 10.10.30.1/24
exit

security passwords default-expired

nat source
  pool UPLINK
    ip address-range 192.168.10.114
  exit
  ruleset SNAT
    to interface gigabitethernet 1/0/1
    rule 8
      match source-address address-range 10.10.20.2-10.10.20.254
      action source-nat pool UPLINK
      enable
    exit
    rule 9
      match source-address address-range 10.10.10.2-10.10.10.254
      action source-nat pool UPLINK
      enable
    exit
    rule 10
      match source-address address-range 10.10.30.1-10.10.30.254
      action source-nat pool UPLINK
      enable
```

```
exit
exit
exit

ip route 0.0.0.0/0 192.168.10.1
ip route 10.10.10.0/24 interface gigabitethernet 1/0/2
ip route 10.10.20.0/24 interface gigabitethernet 1/0/2
ip route 10.10.30.0/24 interface gigabitethernet 1/0/4

ip ssh server

ntp enable
ntp broadcast-client enable

licence-manager
  host address elm.eltex-co.ru
exit
```

ВЫВОДЫ ПО ГЛАВЕ

- Кратко описан протокол внутренней маршрутизации OSPF, который позволяет маршрутизаторам обмениваться маршрутной информацией внутри одной автономной системы.
- Приведен перечень команд для настройки и проверки динамической маршрутизации в туннелях между узлами сети
- Созданы полноценные L3-VPN туннели для связности центрального узла сети и двух филиалов

Глава 11. Заключительная глава. Итоги и пути дальнейшего

Поздравляем! Вы прошли длинный и насыщенный путь от первоначального знакомства с виртуальной средой GNS3 и маршрутизатором vESR до построения сложной защищенной сети корпоративного уровня с динамической маршрутизацией.

Давайте подведем итоги проделанной работы и структурируем полученные вами знания и навыки.

От виртуального образа к сложной корпоративной сети с динамической маршрутизацией

1. **Основа основ.** Вы начали с создания и настройки виртуального образа vESR в GNS3, освоили базовые операции симулятора и подключение к консоли маршрутизатора. Это фундаментальный навык, без которого невозможна любая дальнейшая работа.
2. **Базовые службы.** Была проведена базовая настройка маршрутизатора: назначение hostname, создание пользователей, настройка интерфейсов и понятие зон безопасности (Security Zones) для разграничения трафика.
3. **Автоматизация и доступ в Интернет.** Вы настроили в vESR сервер DHCP, что является стандартом для любой современной локальной сети, и организовали доступ клиентов в Интернет с помощью Source NAT (SNAT). Это типичный сценарий для малого офиса или домашней сети.
4. **Безопасное управление.** Была обеспечена безопасность удаленного управления через настройку сервера SSH и гибкой политики доступа к нему из различных сетевых зон.
5. **Публикация сервисов.** Вы освоили механизм Destination NAT (DNAT), который позволяет открывать доступ к внутренним сетевым ресурсам (например, SSH-серверу) извне, перенаправляя трафик с внешнего "белого" IP-адреса на внутренний "серый".
6. **Объединение сетей.** Для связи изолированных локальных сетей филиалов через ненадежную сеть Интернет был построен GRE-туннель. Вы научились настраивать его параметры, назначать IP-адреса туннельным интерфейсам и прописывать статические маршруты для направления трафика через туннель.
7. **Защита данных.** Надежность — это не только доступность, но и конфиденциальность. Туннель GRE был усилен криптографической защитой с помощью IPsec, создав полноценный защищенный канал (GRE over IPsec). Вы настроили политики IKE и IPsec, общие ключи и обеспечили шифрование всего трафика между узлами.
8. **Масштабирование инфраструктуры.** Вы расширили сеть, добавив второй филиал, и подготовили инфраструктуру для размещения и публикации веб-

сервиса, повторив и закрепив пройденные этапы настройки. Это продемонстрировало тиражируемость и масштабируемость предложенных решений.

9. **Динамическая маршрутизация OSPF.** Венцом построения отказоустойчивой сети стала замена статических маршрутов на динамический протокол OSPF. Вы настроили обмен маршрутной информацией между всеми узлами сети через защищенные туннели, создав полноценные L3VPN. Теперь сеть может автоматически адаптироваться к изменениям, а маршруты между филиалами и центральным офисом устанавливаются и поддерживаются автоматически.

vESR и GNS3: Идеальный тандем для обучения

В ходе работы вы на практике убедились в преимуществах связки GNS3 и vESR:

- **Доступность:** Полнофункциональная лаборатория разворачивается на обычном ПК.
- **Гибкость:** Легко создавать и изменять даже сложные сетевые топологии.
- **Реализм:** vESR — это не упрощенный симулятор, а практически полный аналог физического оборудования Eltex ESR, использующий тот же код и синтаксис команд.
- **Безрисковость:** Любую ошибку в конфигурации можно мгновенно исправить, а "упавшее" устройство — перезагрузить.

Что дальше? Рекомендации для дальнейшего изучения

Полученная база открывает дорогу к освоению более сложных и востребованных сетевых технологий. Для дальнейшего самостоятельного изучения на вашей уже развернутой лабораторной базе мы рекомендуем:

1. **Углубленное изучение OSPF.** Поэкспериментируйте с multi-area OSPF, настройкой стоимостей маршрутов (cost), аутентификацией между OSPF-соседями и виртуальными линками (Virtual Link).
2. **Отказоустойчивость.** Изучите и настройте протокол VRRP на маршрутизаторах vESR для обеспечения резервирования шлюза по умолчанию в локальной сети.
3. **Качество обслуживания (QoS).** Опытным путем настройте политики QoS для приоритизации голосового трафика (VoIP) или видео над обычным веб-трафиком внутри туннелей GRE.
4. **MPLS.** Виртуальный маршрутизатор vESR поддерживает MPLS. Попробуйте построить простую MPLS L3VPN между филиалами — золотой стандарт для построения сетей крупных предприятий. Это следующий логический шаг после GRE over IPsec.

5. **BGP.** Для связи с другими автономными системами (например, с другим провайдером или в дата-центре) изучите и настройте протокол BGP на маршрутизаторе vESR.
6. **Скриптование и автоматизация.** Используйте Python и библиотеки вроде Netmiko или Paramiko для автоматизации рутинных операций конфигурирования ваших vESR (массовая смена паролей, сбор конфигураций, применение шаблонов).

Заключение

Это руководство помогло вам не просто познакомиться с еще одним сетевым устройством, а системно подойти к построению современной сетевой инфраструктуры. Вы прошли весь путь — от настройки базовых параметров маршрутизатора до построения распределенной защищенной сети с динамической маршрутизацией, объединяющей центральный офис и удаленные филиалы.

Вы освоили не отдельные команды, а логику и взаимосвязь ключевых сетевых сервисов: от раздачи IP-адресов до организации защищенных магистральных каналов и интеллектуальной динамической маршрутизации.

Полученные знания и навыки являются прочным фундаментом для работы не только с оборудованием Eltex, но и с маршрутизаторами других вендоров, а также для подготовки к профессиональным сертификациям. Помните, что мастерство приходит с практикой. Не бойтесь экспериментировать, ломать и чинить созданные вами сети в безопасной виртуальной среде GNS3.

Удачи в дальнейшем изучении бесконечно интересного мира сетевых технологий

Список литературы

Список использованной литературы и ссылок

1. https://eltexcm.ru/catalog/servisnye-marshrutizatory/virtualnyj-servisnyj-marshrutizator-vesr/virtualnyj-servisnyj-marshrutizator-vesr.html?utm_medium=cpc&utm_source=yandex&utm_campaign=78721658&utm_content=cid%7C78721658%7Cgid%7C5209140120%7Caid%7C14280994877%7Cadp%7Cno%7Cdvc%7Cdesktop%7Cpid%7C45034055164%7Crid%7C45034055164%7Cdid%7C45034055164%7Cpos%7Cpremium1%7Cadn%7Csearch%7Ccid%7C0%7C&utm_term=vESR&roistat_referrer=none&roistat_pos=premium_1&roistat=direct6_search_14280994877_vESR&yclid=3607976104414674943
2. <https://docs.eltex-co.ru/ede/initial-router-configuration-380863579.html>
3. <https://docs.eltex-co.ru/display/ED23/Quick+Start+vESR>
4. <https://github.com/GNS3/gns3-gui/releases>
5. <https://docs.gns3.com/docs/getting-started/installation/windows/>
6. https://github.com/alekho/EVE-NG_vESR/blob/main/README.md
7. <https://chat.deepseek.com/>
8. https://sysahelper.gitbook.io/sysahelper/main/telecom/main/basic_setting
9. <https://serverspace.ru/support/glossary/nat/>
10. <https://mentoring.digital/blog/chto-takoe-nat-i-dlya-chego-on-nuzhen:-ponimanie-osnov-setevoy-tehnologii>
11. <https://habr.com/ru/companies/otus/articles/779970/>
12. <https://docs.gns3.com/docs/using-gns3/beginners/import-gns3-appliance/>
13. <https://newstorial.comexpertnetworkconsultant.comdocs.selectel.ru>

14. <https://newstorial.com>

15. <https://putty.org.ru/download>

Приложение

- [Конфигурационный файл виртуального маршрутизатора vesr124-1.](#)
- [Конфигурационный файл виртуального маршрутизатора vesr124-2.](#)
- [Конфигурационный файл виртуального маршрутизатора vesr124-3.](#)
- [Конфигурационный файл виртуального маршрутизатора vesr124-4.](#)