1. Настройка удалённого доступа SSH в маршрутизаторе vESR.

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](https://eltex-co.ru/catalog/service_gateways/virtualnyy_servisnyy_marshrutizator_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 безплатных 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 строчки, 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 выгляди так:

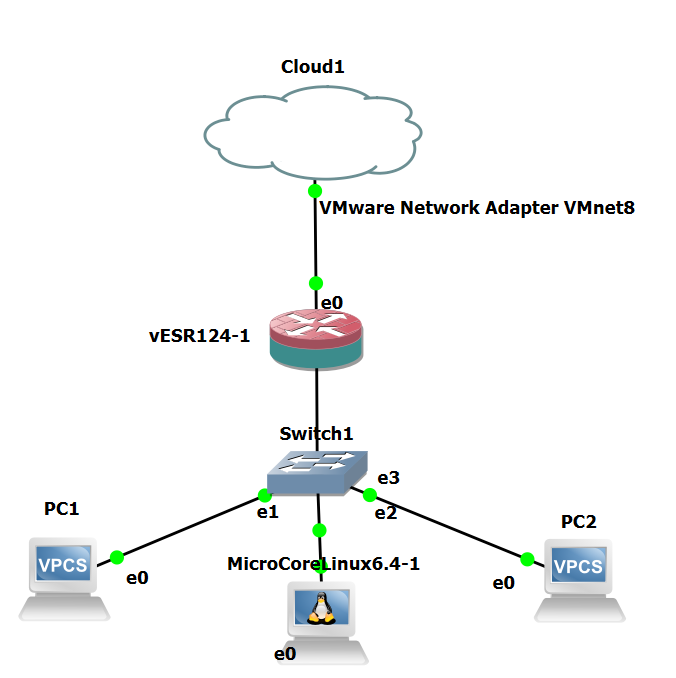


Рис. Копия экрана со схемой стенда.

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:

vesr-1# configure

vesr-1(config)# security zone-pair trusted self

vesr-1(config-zone-pair)# rule <number>

vesr-1(config-zone-rule)# action permit

vesr-1(config-zone-rule)# match protocol tcp

vesr-1(config-zone-rule)# match source-address <network object-group>

vesr-1(config-zone-rule)# match destination-address <network object-group>

vesr-1(config-zone-rule)# match source-port any

vesr-1(config-zone-rule)# match destination-port <service object-group>

vesr-1(config-zone-rule)# enable

vesr-1(config-zone-rule)# exit

vesr-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 vesr-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

vesr-1# config

vesr-1(config)# object-group service ssh

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

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

vesr-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

vesr-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

vesr-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

vesr-1(config)# security zone-pair trusted self

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

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

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

vesr-1(config-security-zone-pair-rule)# match source-address object-group LAN\_GATEWAY

vesr-1(config-security-zone-pair-rule)# match destination-address object-group LAN

vesr-1(config-security-zone-pair-rule)# match source-port any

vesr-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

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

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

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

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

vesr-1(config)# 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

vesr-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

vesr-1(config)# do save

Configuration has been successfully saved

vesr-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 \*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

vesr-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 обьектов WAN нужно ещё добавить группу клиентов SSH:

vesr-1# config

vesr-1(config)#object-group network clients

vesr-1(config-object-group-network)# ip address-range 192.168.10.0-192.168.10.254

vesr-1(config-object-group-network)# exit

vesr-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 vesr-1, полученный командой sh ip int)  по протоколу SSH:

vesr-1(config)# security zone-pair untrusted self

vesr-1(config-security-zone-pair)# rule 10

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

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

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

vesr-1(config-security-zone-pair-rule)# match source-address objec

t-group clients

vesr-1(config-security-zone-pair-rule)# match destination-address

object-group WAN

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

ject-group ssh

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

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

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

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

vesr-1(config)#do commit

vesr-1(config)#do confirm

vesr-1(config)#exit

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

vesr-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

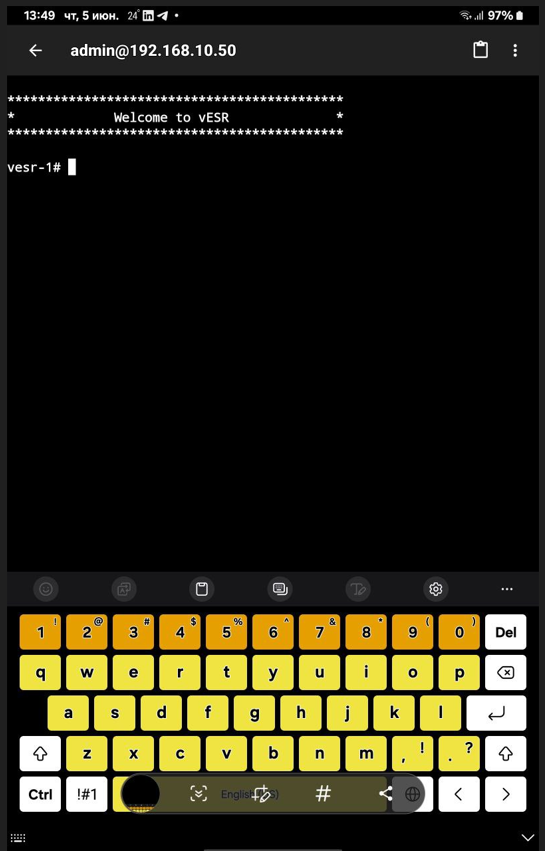
2025-06-05T10:47:01+00:00 %AAA-LOCAL-I-SESSION: ssh: session opened for user admin

vesr-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.



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 \*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

vesr-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