Инцидент № C0001

Дата создания: 21.07.2021

Дата последней корректировки: __26.01.2022_

Инструкция по реагированию на инциденты, решением которых является переустановка или установка dst файла на Coordinator.

Этап 1. Подготовка оборудования.

Для установки/переустановки dst файла потребуется:

- Физический доступ к Coordinator HW
- Питание к Coordinator HW
- Монитор с VGA разъемом
- Питание к монитору
- Клавиатура
- Кабель VGA
- USB-flash накопитель в формате FAT32, ext2, ext3 или ext4.

Этап 2. Настройка координатора

Этап 2.1. Сброс ключевой информации координатора[1]

При запуске Coordinator HW операционная система запросит логин и пароль. Слева от login имя координатора, данное ему при предыдущей установке. При вводе пароля символы не отображаются.

Login	user
Password	«в .xps файле»

Рисунок 1

После успешной авторизации под user, требуется повысить права командой *enable*. Потребуется ввести пароль администратора. Если он Вам неизвестен, то уточните его у Администратора сети. После успешного повышения прав “>” заменяется на “#”.

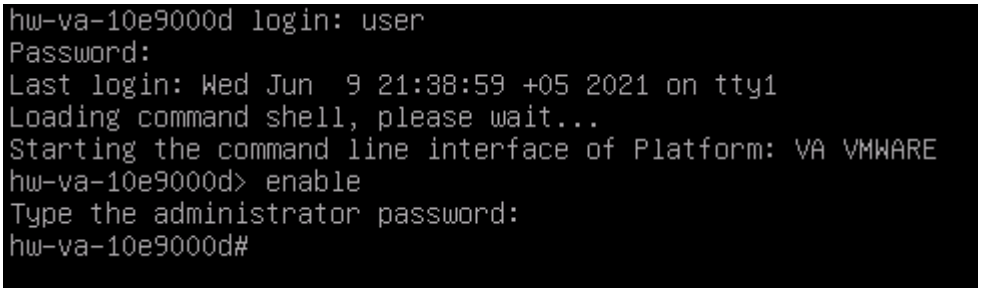

Рисунок 2

Для удаления ключевой информации необходимо ввести команду *admin remove keys*. Далее на экране отобразится предупреждающее сообщение. Для продолжения удаления необходимо согласиться с заглавной буквы (Yes).

[1] Данный этап пропускается в случае, если Ваш корд был получен вами после ремонта. Приступите к настройке сразу с этапа 2.2.

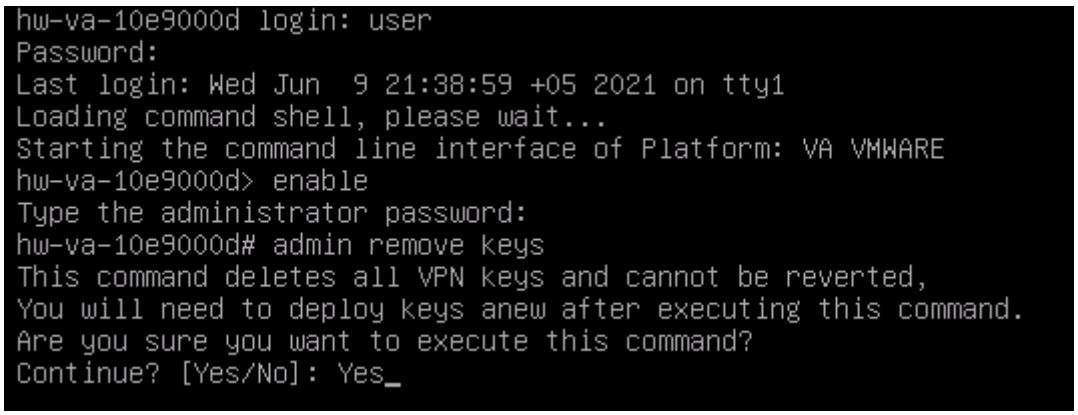

Рисунок 3

После согласия начнется процесс удаления.

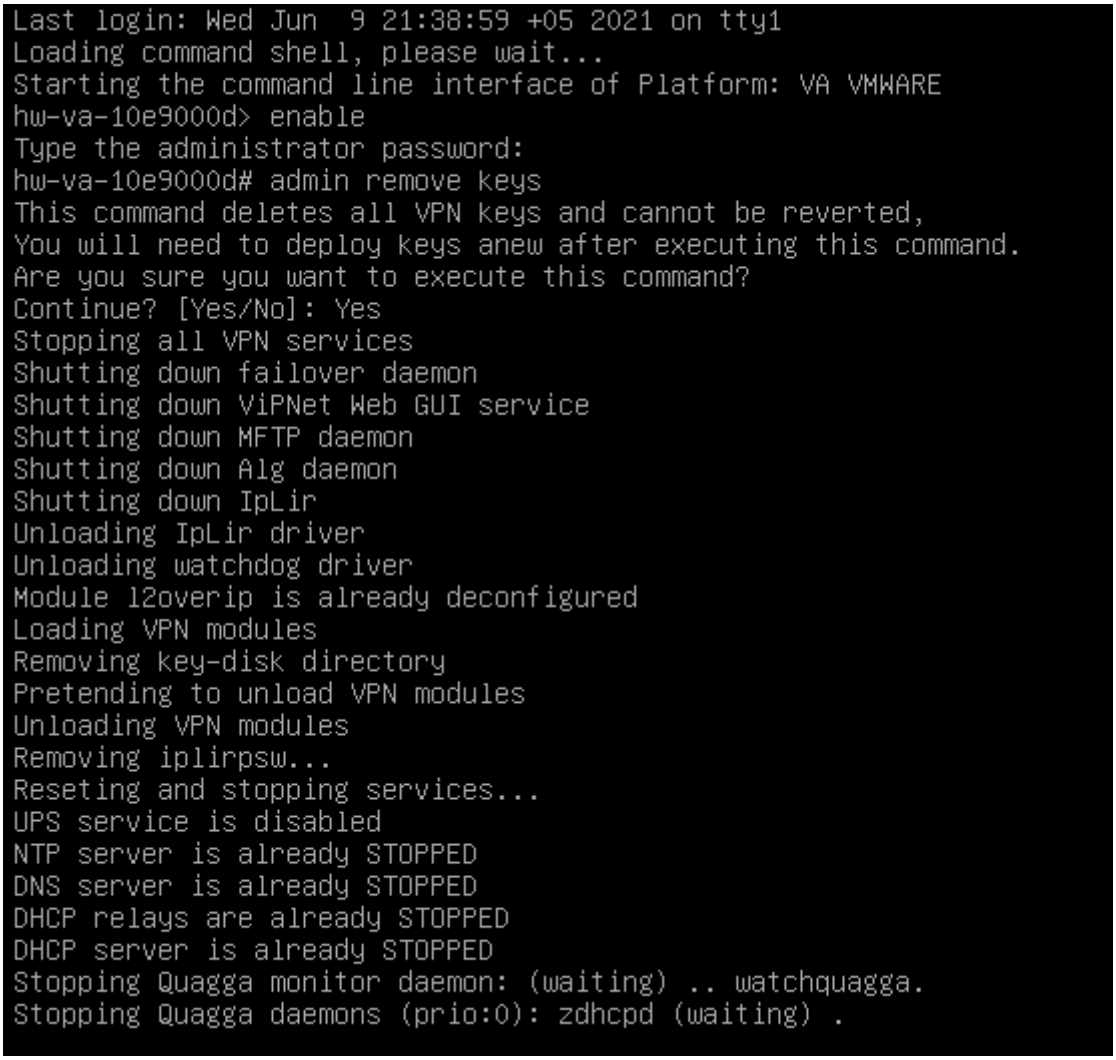

Рисунок 4

После успешного удаления система может перезагрузиться и запросить login как в начале следующего этапа. Если все произошло успешно, можно переходить к Этапу 2.2.

Этап 2.2. Настройка координатора с нуля.

При первоначальной инициализации координатора или после удаления ключевой информации координатор имеет базовое имя и базовую пару логин-пароль. Стоит отметить, что имя

координатора по умолчанию зависит от модели.

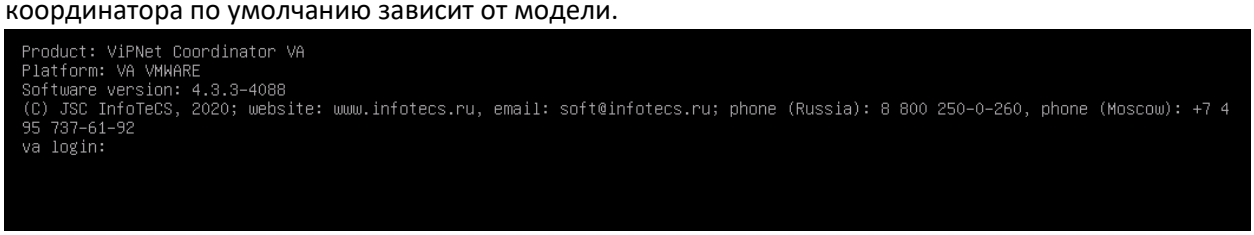

Рисунок 5

Login	user
Password	user

После успешной авторизации система предоставит на выбор два варианта настройки координатора:

1. В командой строке
2. Псевдографический интерфейс

В данной инструкции используется второй вариант. Для выбора достаточно ввести соответствующую цифру.

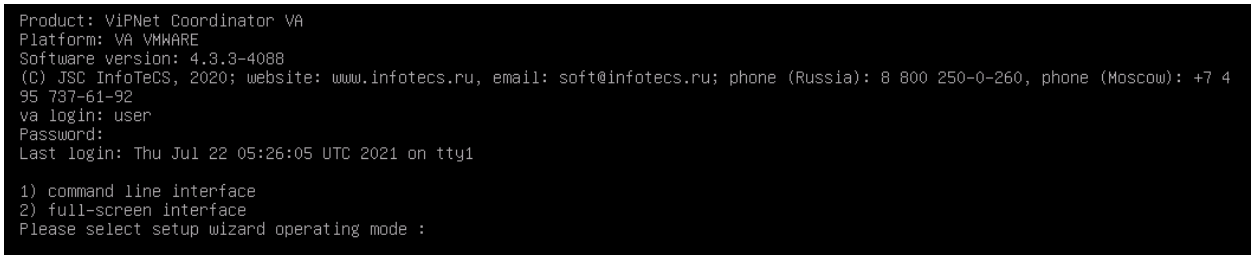

Рисунок 6

Дальнейшие действия будут в соответствии со скриншотами. В необходимых случаях будут даны комментарии.

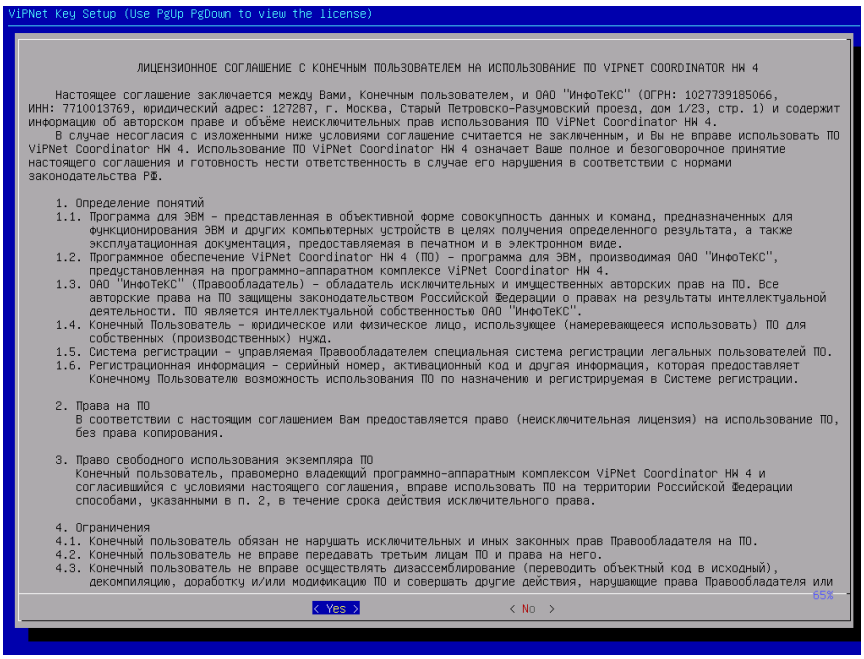

Рисунок 7

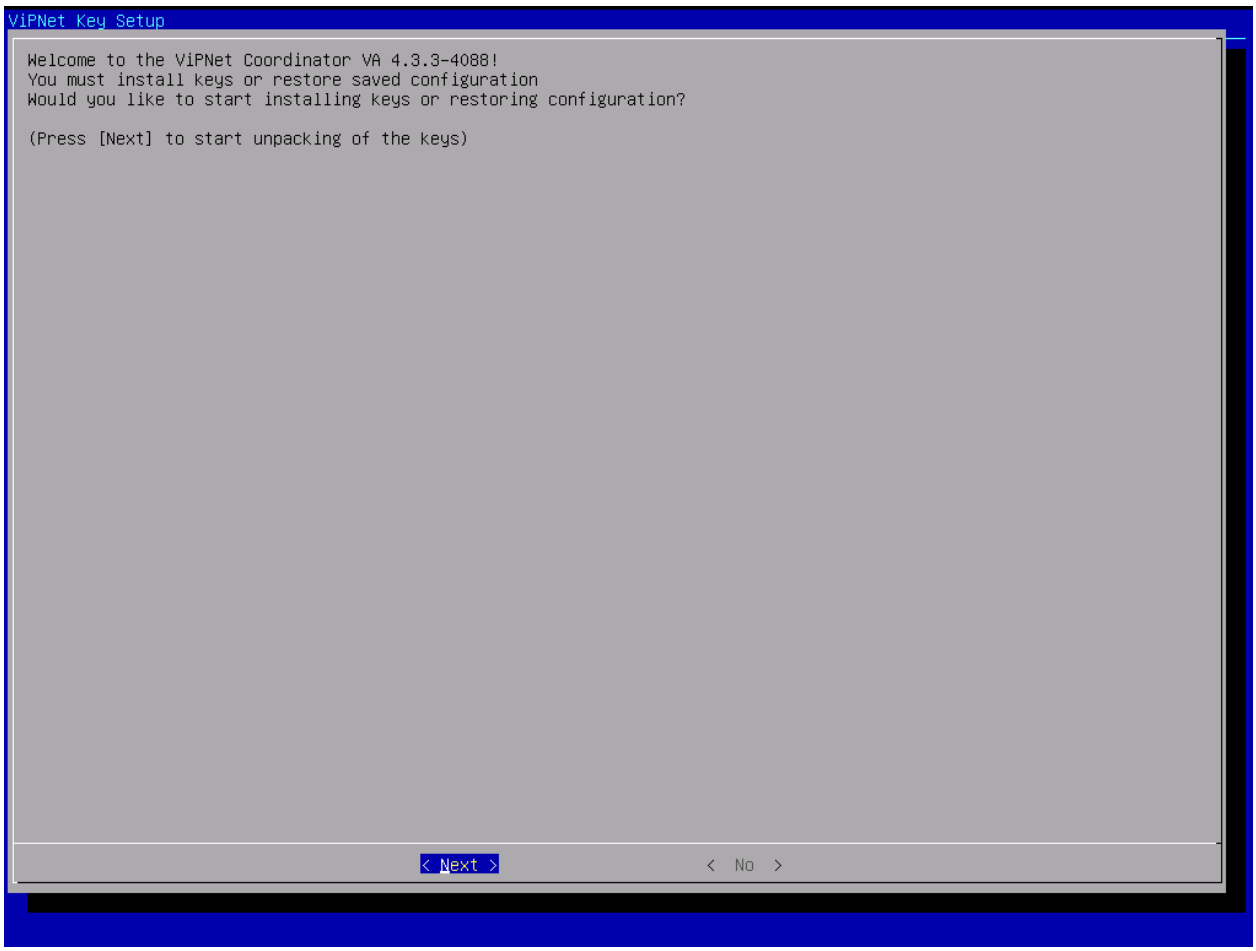

Рисунок 8

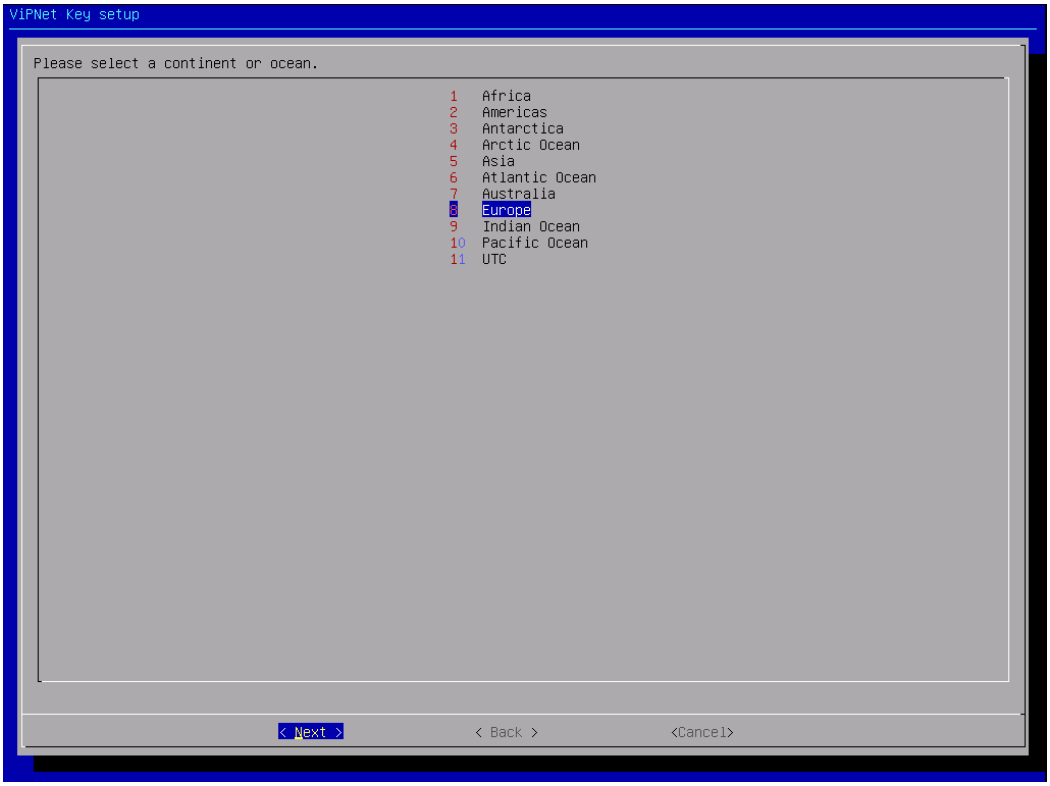

Рисунок 9

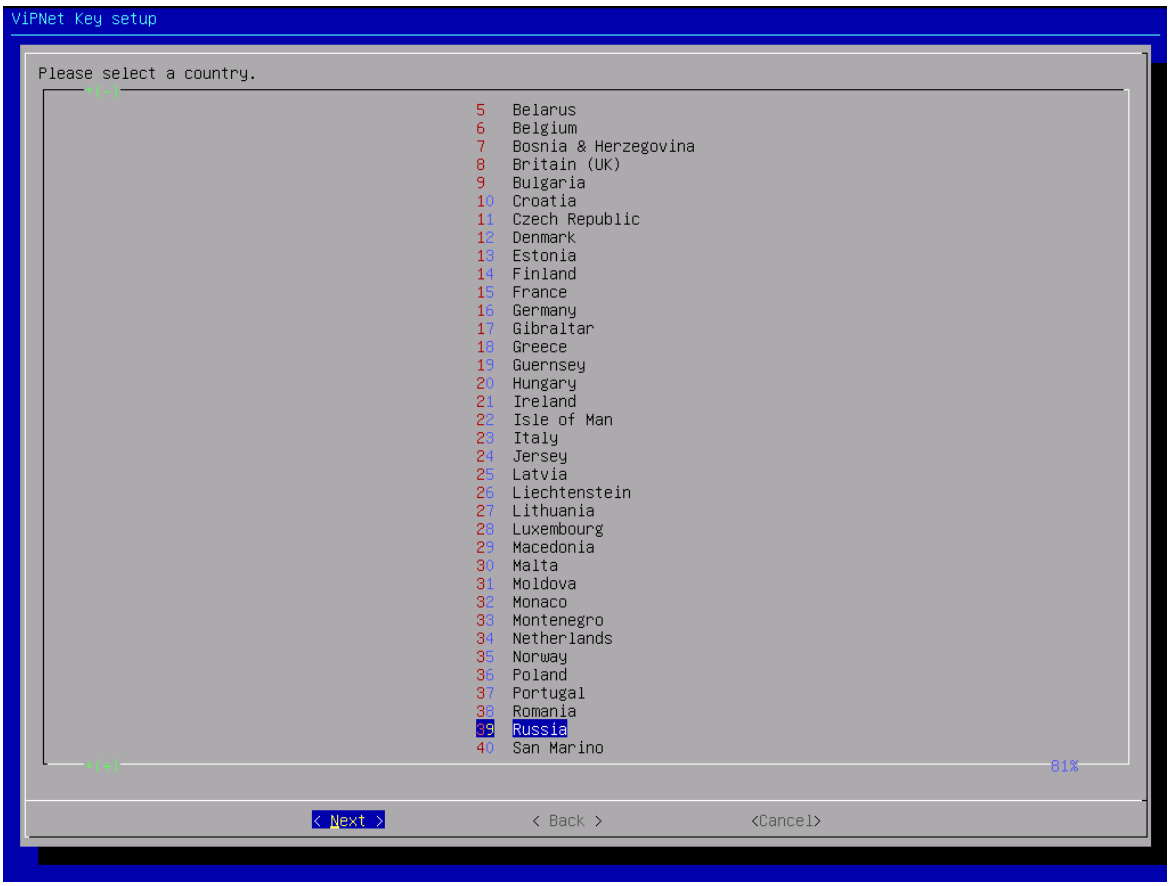

Рисунок 10

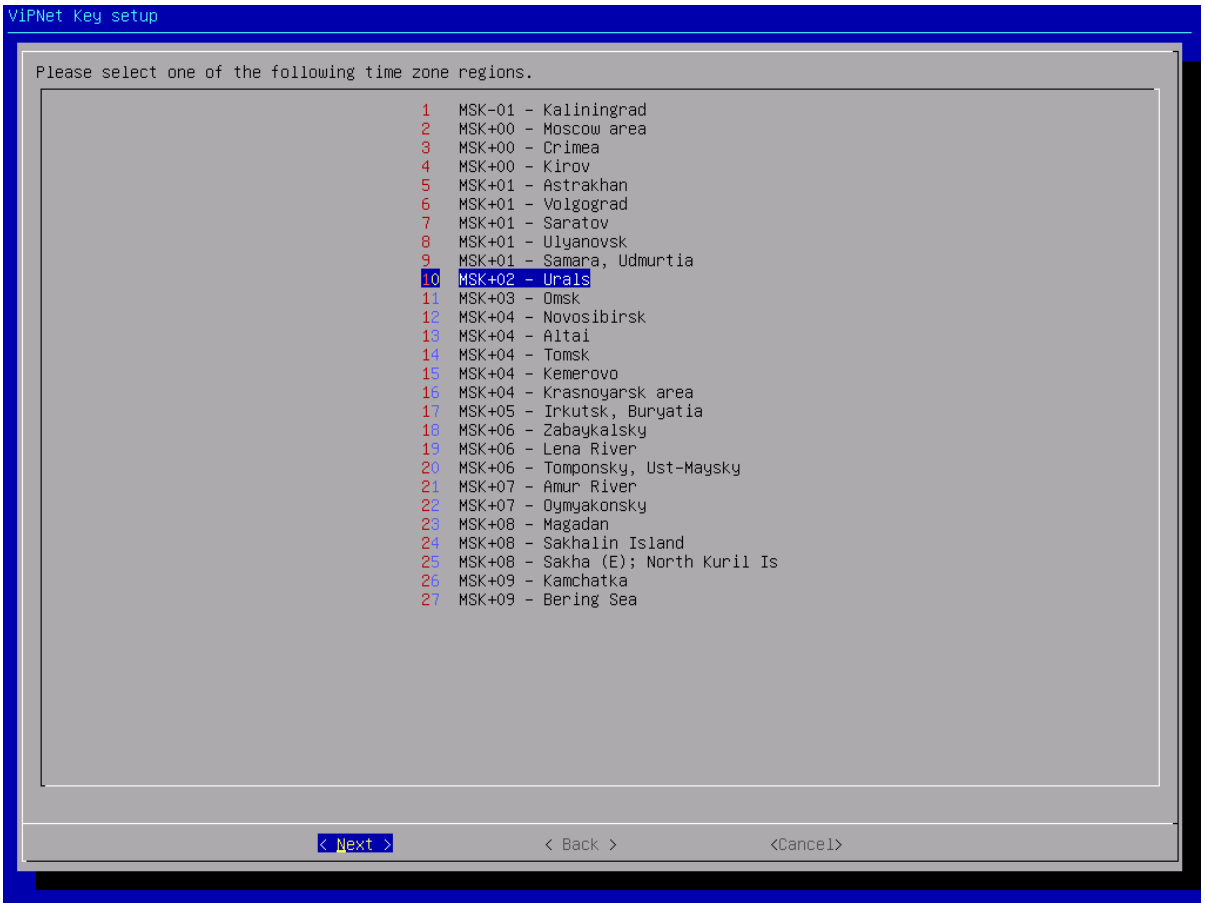

Рисунок 11

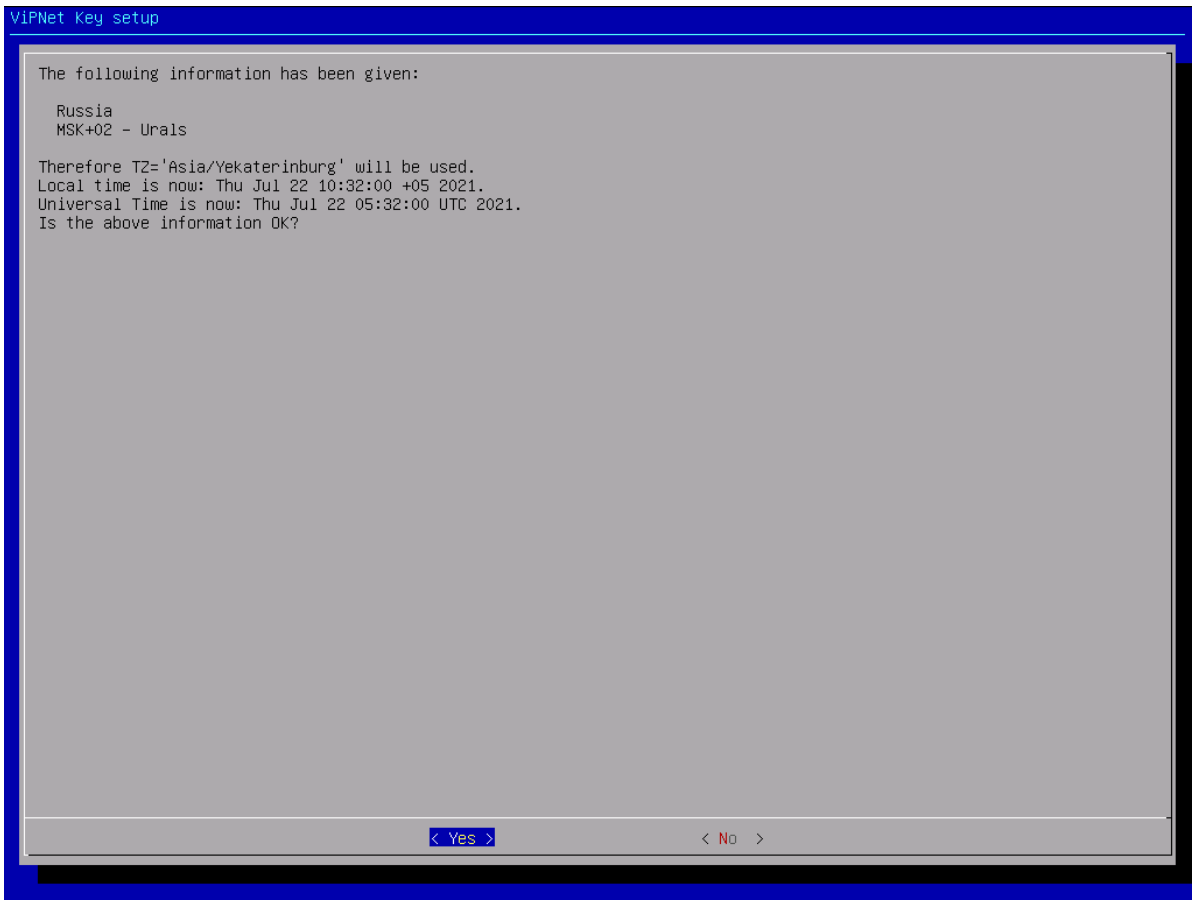

Рисунок 12

Очень важно, что бы на координаторе были правильно настроены дата и время.

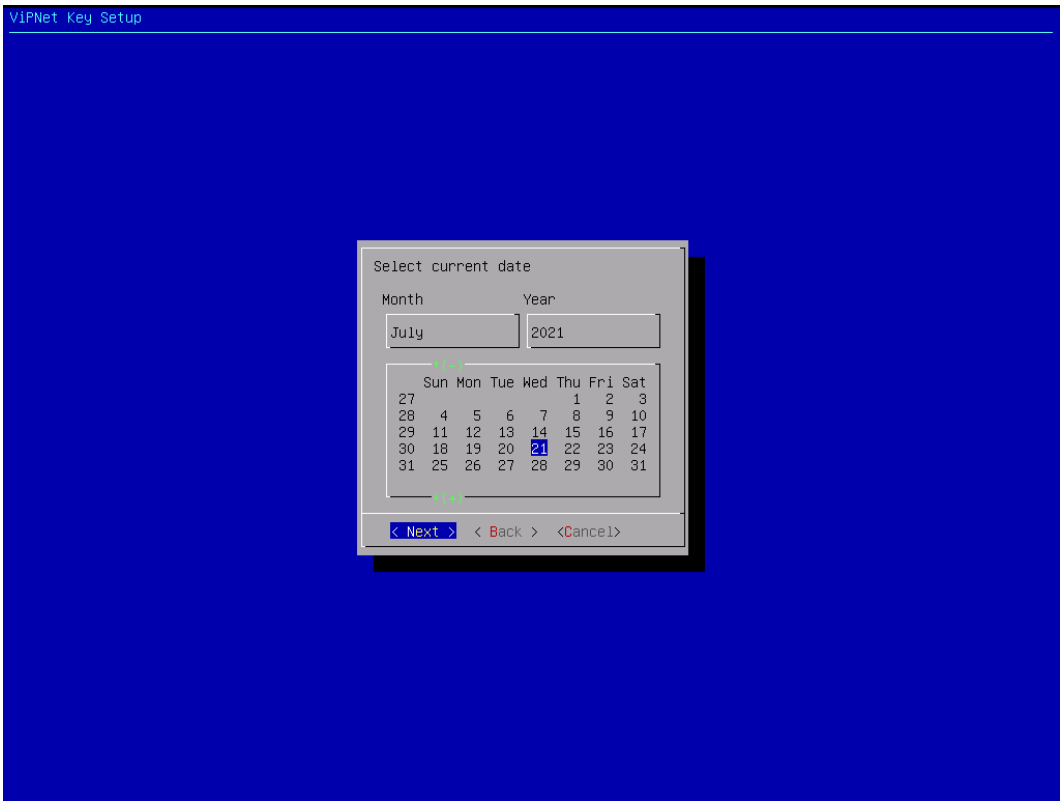

Рисунок 13

Рисунок 14

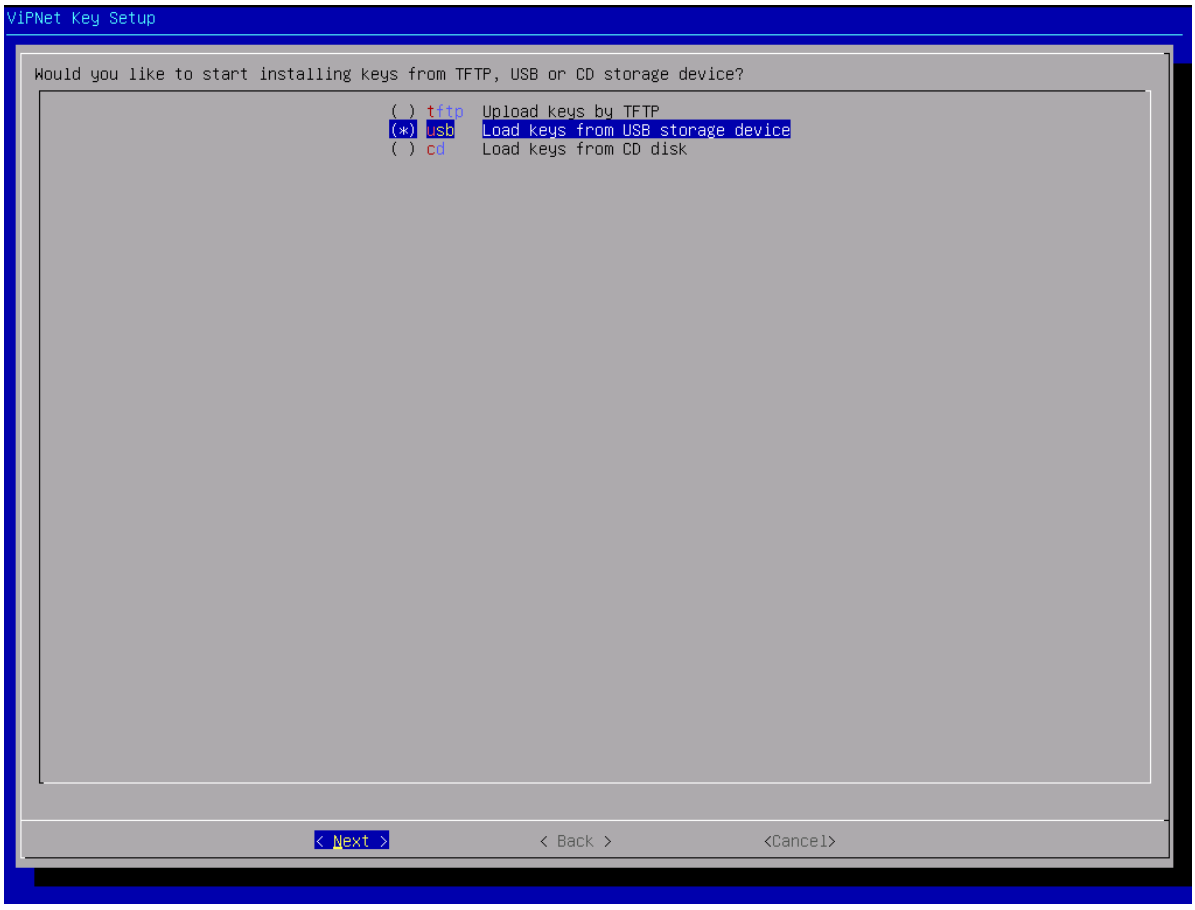

Рисунок 15

Если все до этого момента было сделано верно, то система попросит Вас вставить usb-flash носитель, на котором хранится *.dst файл.

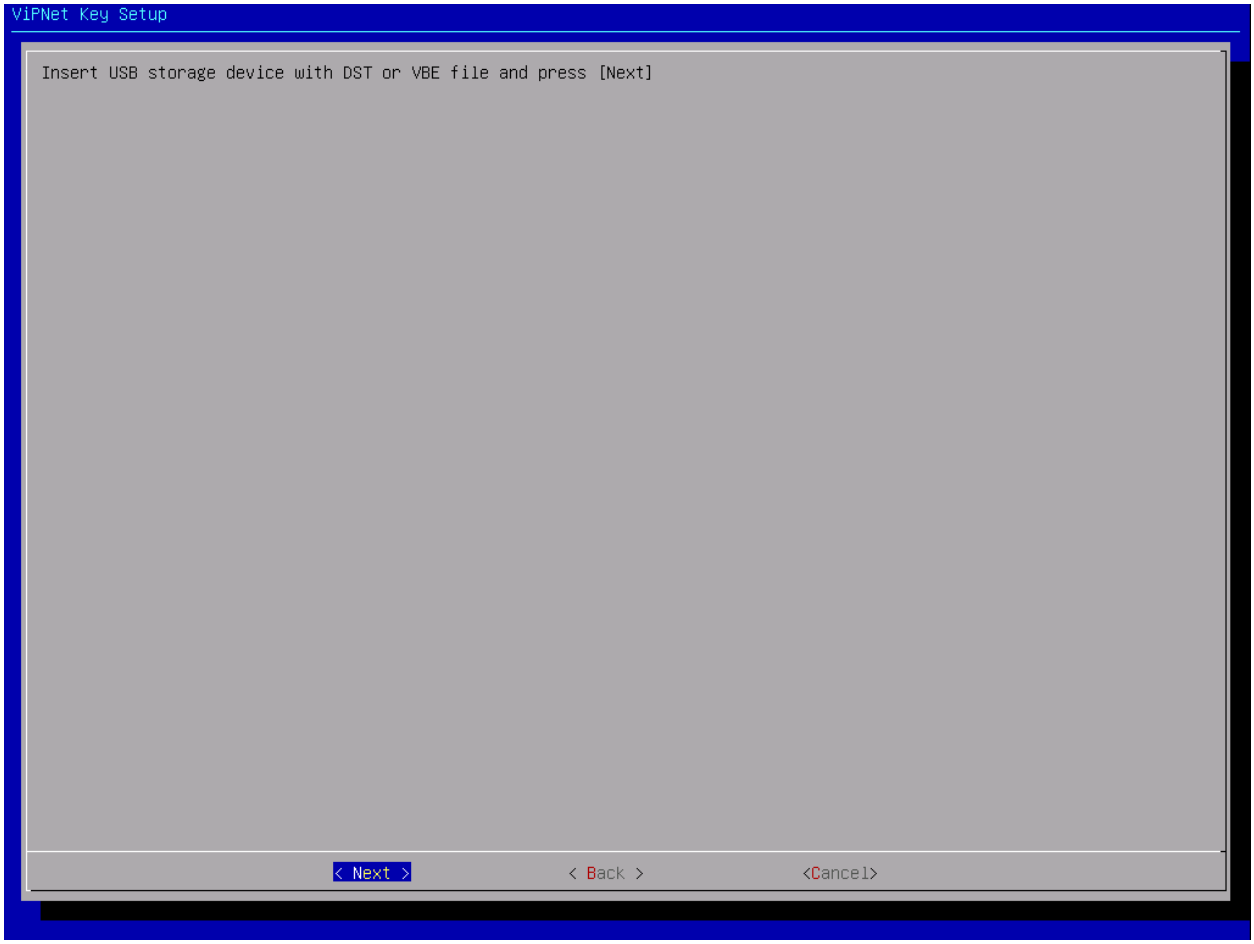

Рисунок 16

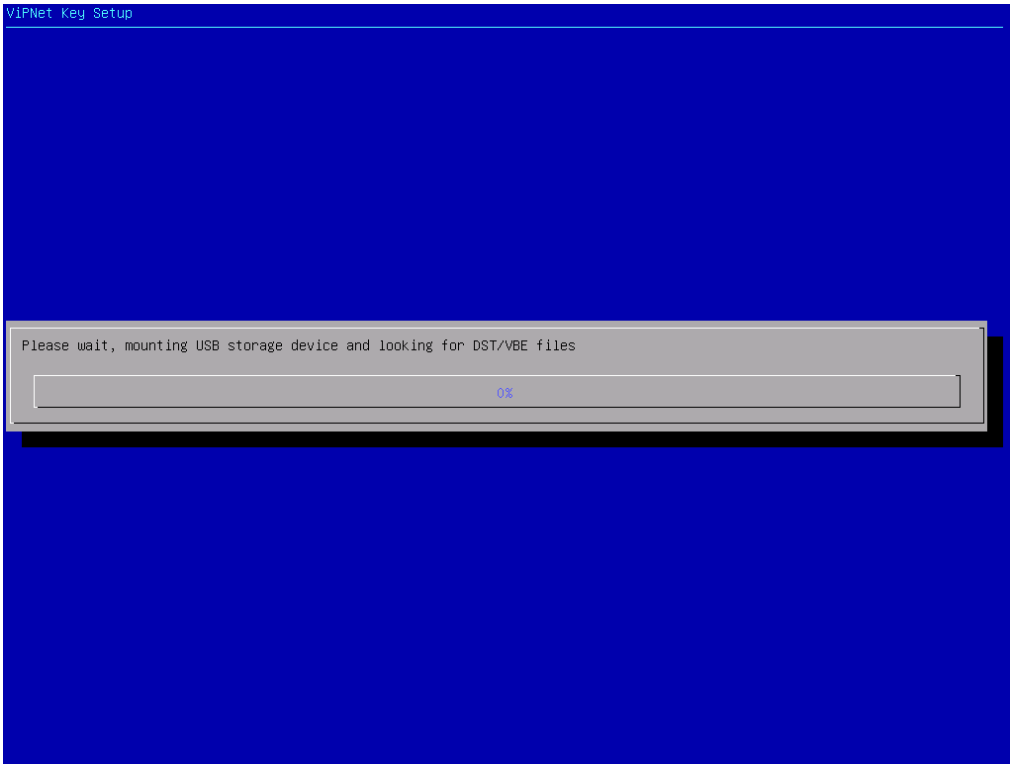

Рисунок 17

Если usb-flash был правильно отформатирован, работает исправно и на нем имеется *.dst файл, то система попросит Вас его выбрать. Выберите соответствующий, а скорее всего единственный файл.

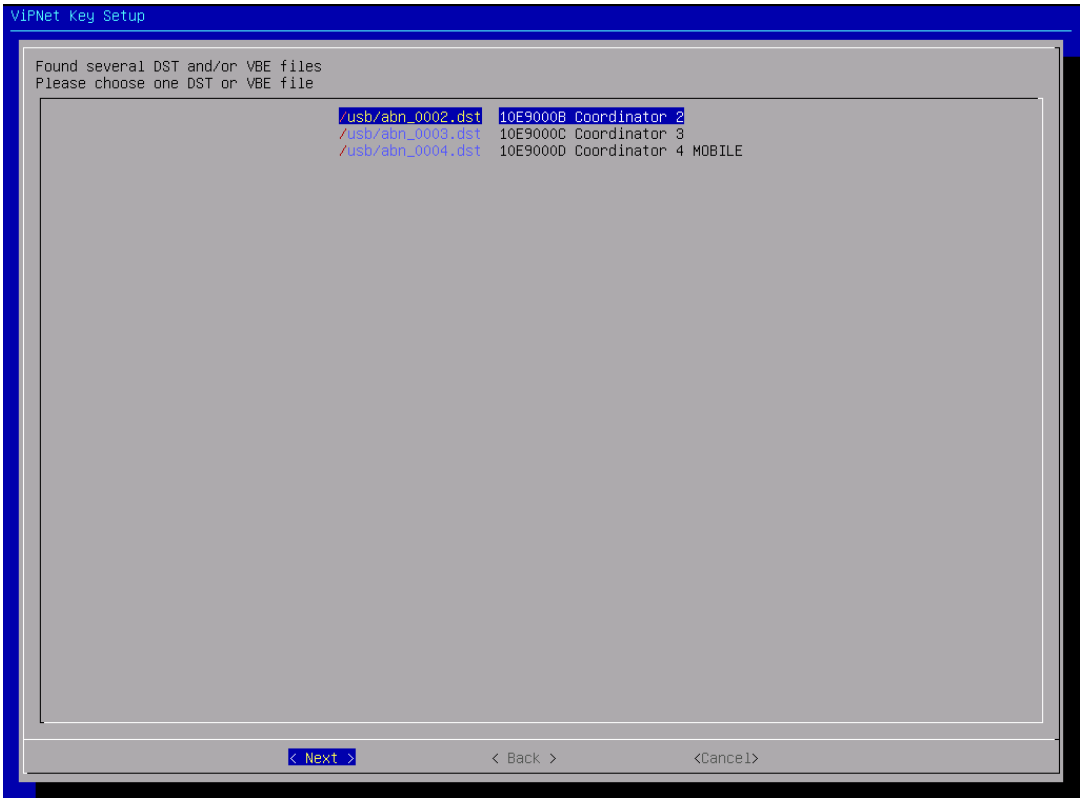

Рисунок 18

После выбора *.dst, система запросит ввести пароль. Данный пароль хранится в *.xps файле, который идет в комплекте с *.dst. Если данного файла нет или он был утерян – обратитесь к Администратору сети.

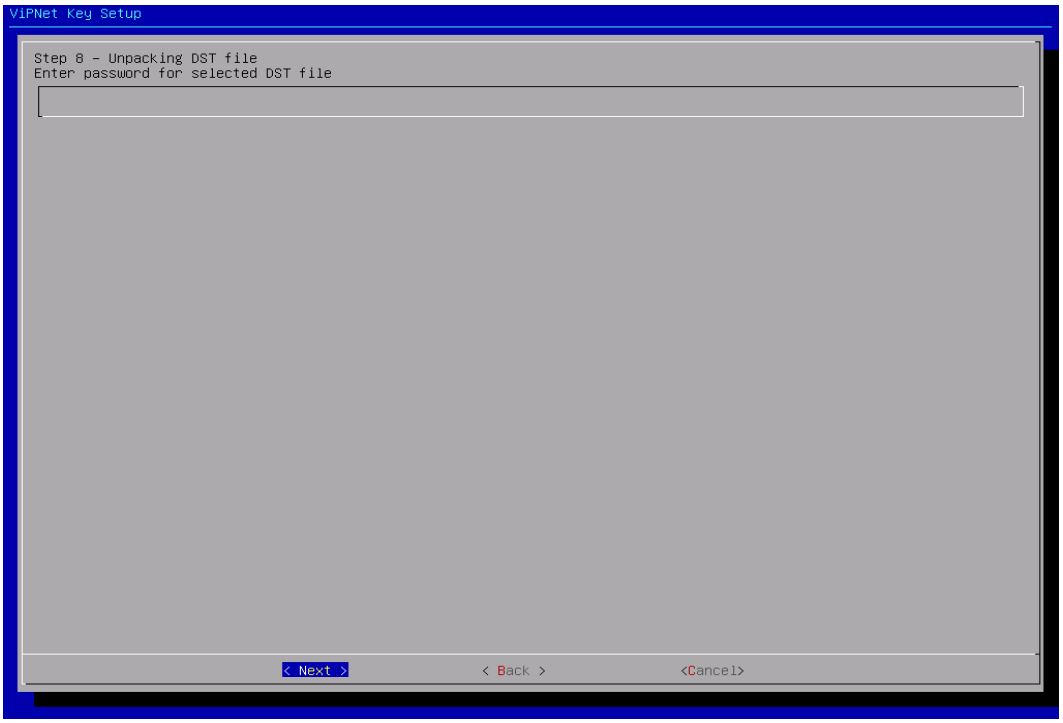

Рисунок 19

После успешного ввода пароля, система может перезагрузиться. После успешного запуска настройка координатора продолжится.

В координаторе может быть несколько портов. В зависимости от модели, их расположение и количество может различаться. В данной инструкции будет использоваться настройка для работы координатора «в разрез». Для реализации данного варианта достаточно настроить 1 (один) сетевой интерфейс(порт). Примерный вариант данной схемы проиллюстрирован на Рисунок 20.

Однако, согласно требованиям регулятора, Вам необходим сертифицированный межсетевой экран. Координатор является сертифицированным межсетевым экраном, но для выполнения требования, он должен быть установлен в разрыв и иметь два настроенных интерфейса – один на вход и второй на выход. К сожалению, мы не можем полностью проинструктировать Вас по этому вопросу, так как многое упирается в настройки вашей локальной сети и на ваше владение предметом.

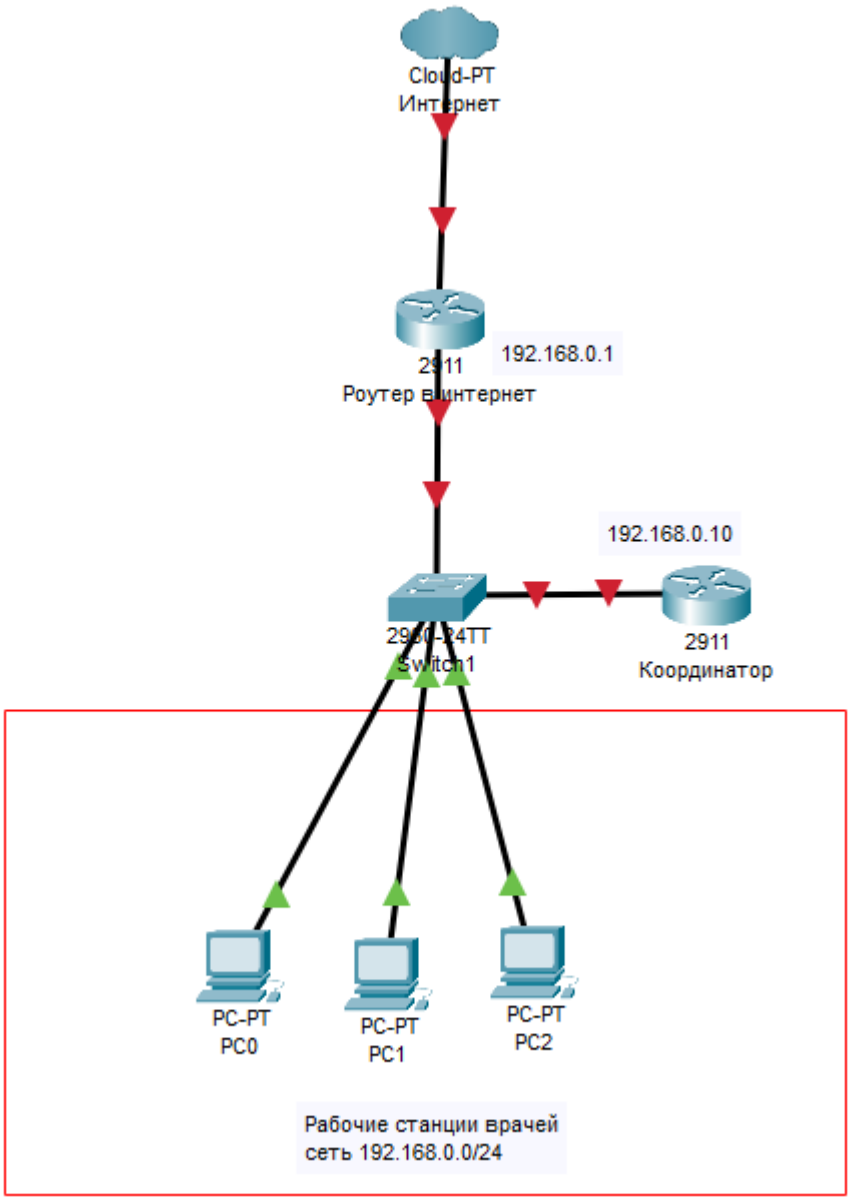

Рисунок 20

В данной инструкции будет настроен сетевой интерфейс eth0. Вы можете настраивать любой удобный для себя сетевой интерфейс. На Рисунок 21 сетевой интерфейс eth0 выбирается

активным, следовательно все другие будут неактивны. Выбор осуществляется клавишей «Пробел».

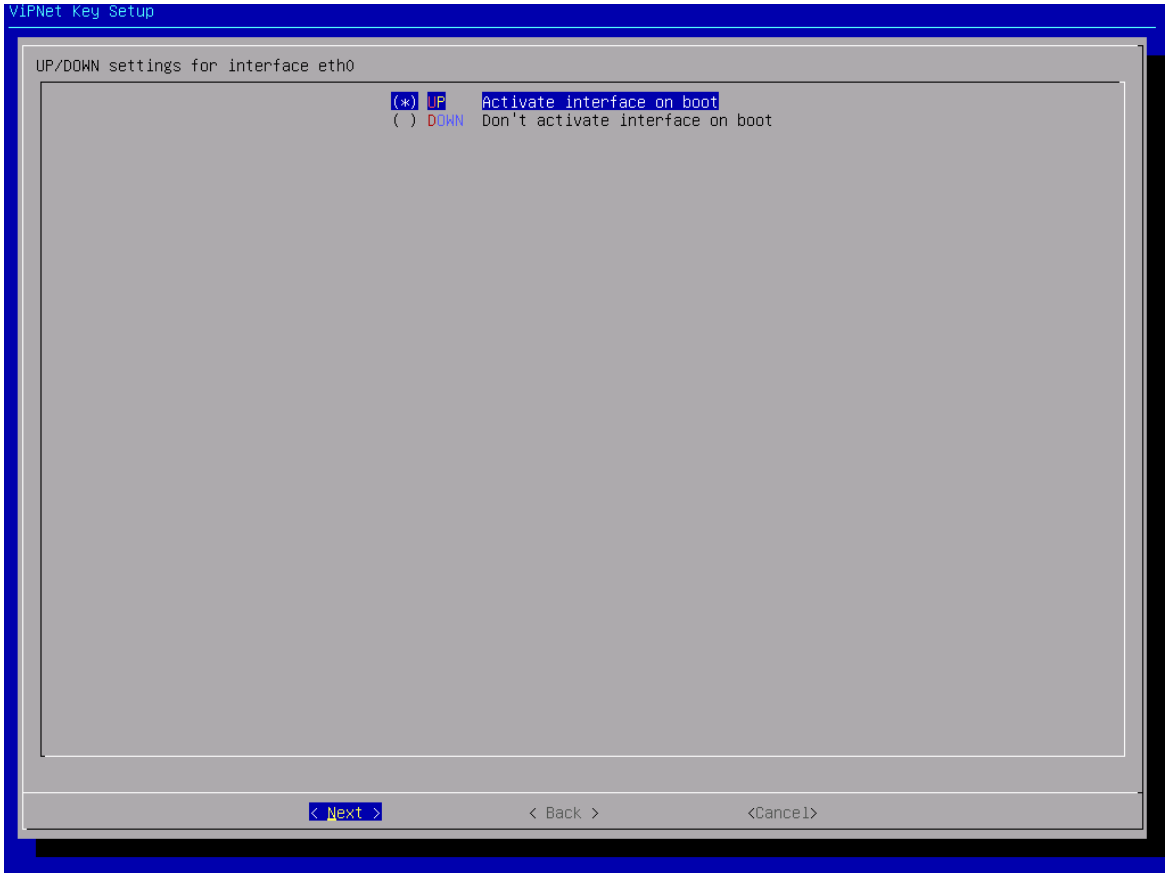

Рисунок 21

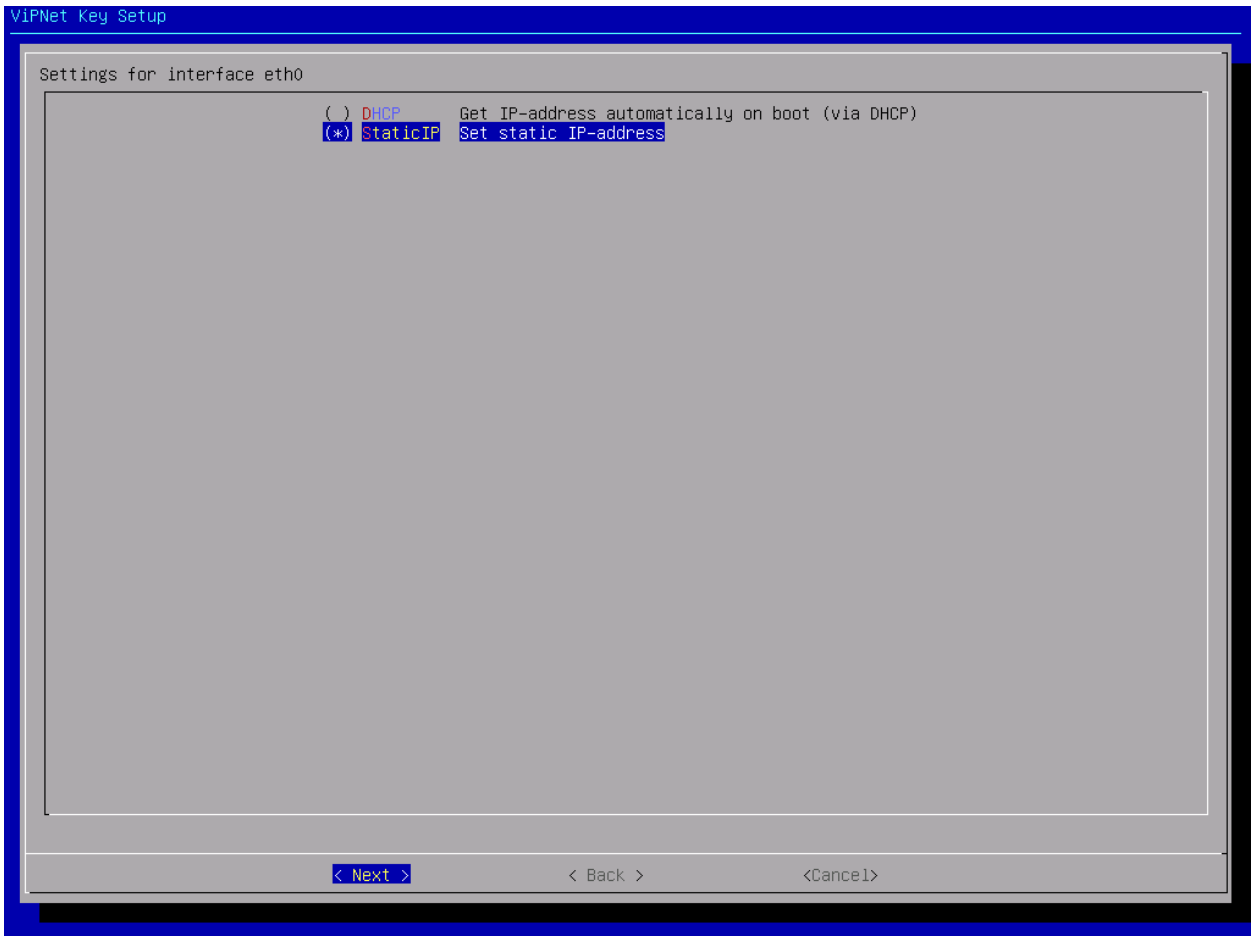

Рисунок 22

На данном шаге (Рисунок 23) указывается IP-адрес координатора и его маска. Настраивать Вы вольны в соответствии со своей сеткой. Адрес на скриншоте указан для примера.

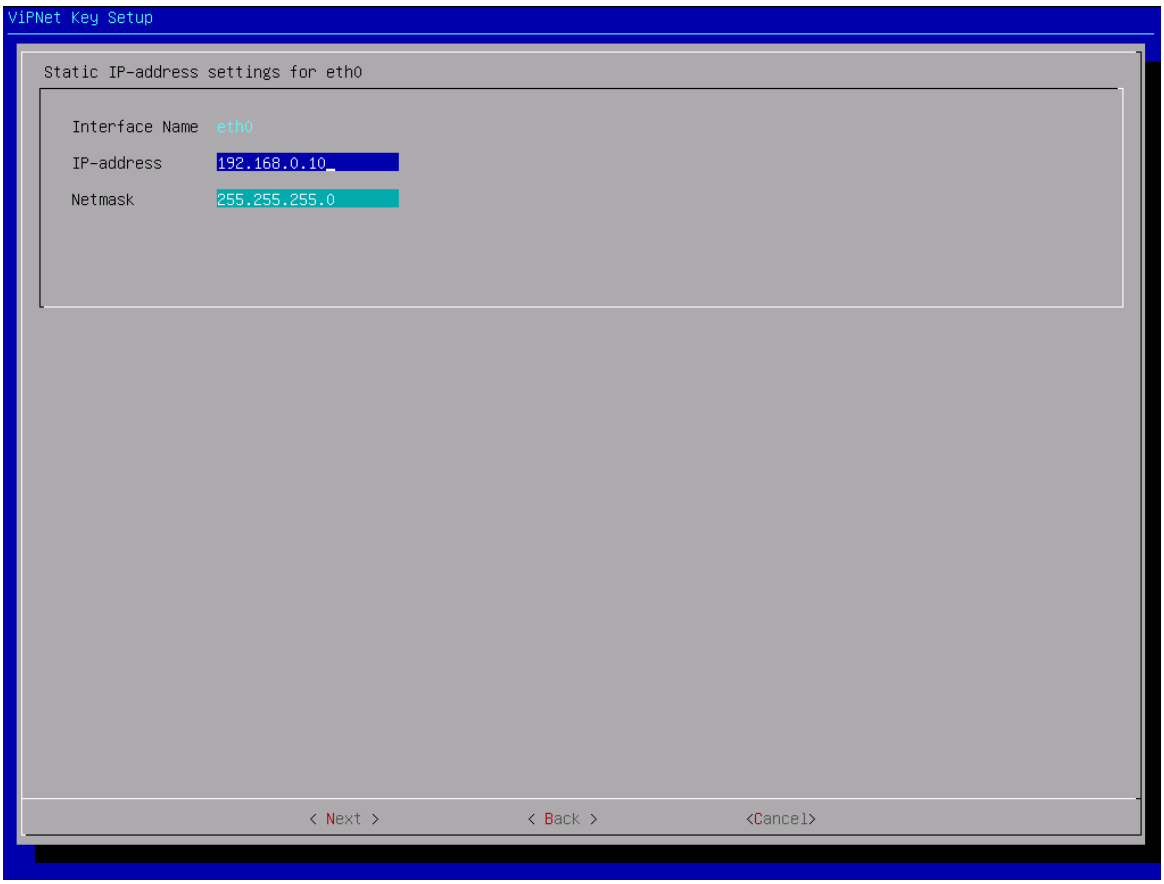

Рисунок 23

Как и говорилось ранее, остальные интерфейсы отключаются.

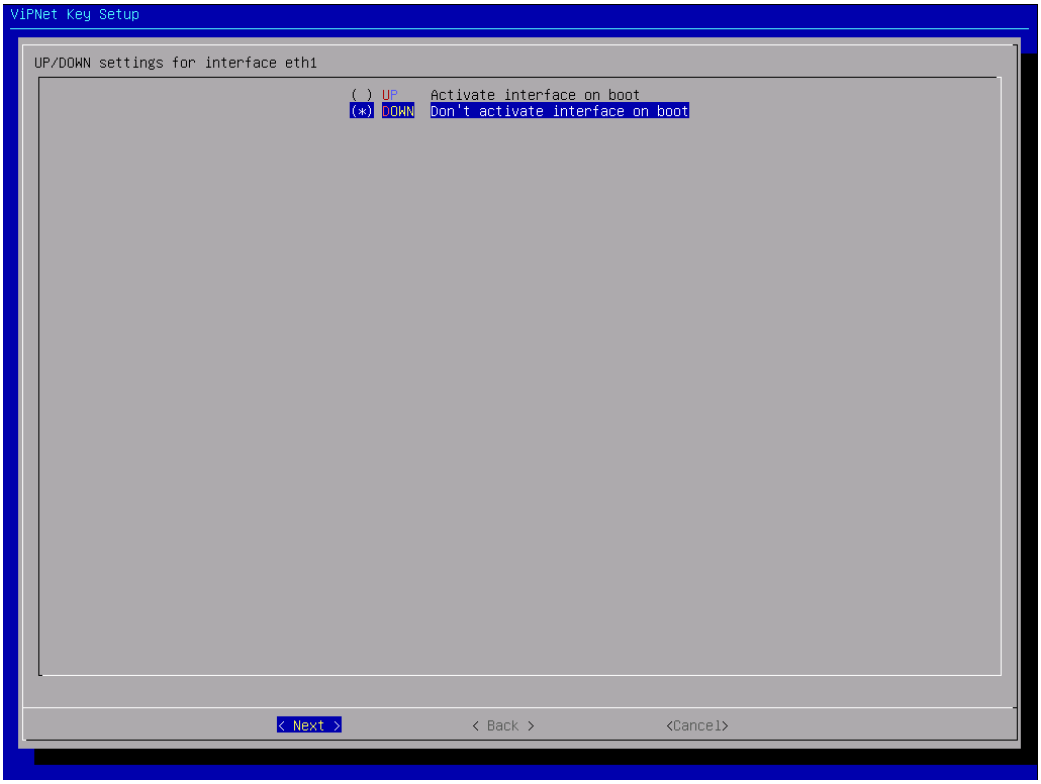

Рисунок 24

На Рисунок 25 указывается маршрут по умолчанию. Здесь следует вписать адрес Вашего роутер, который подключен к координатору.

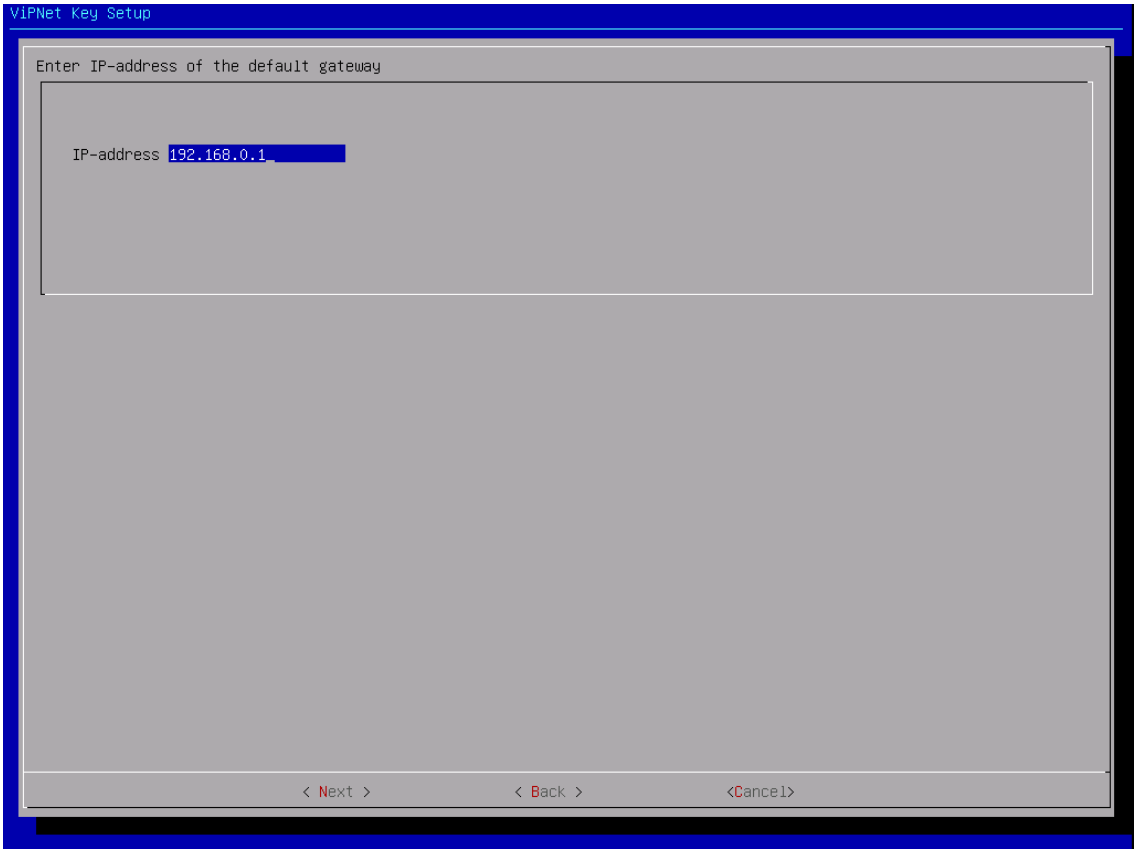

Рисунок 25

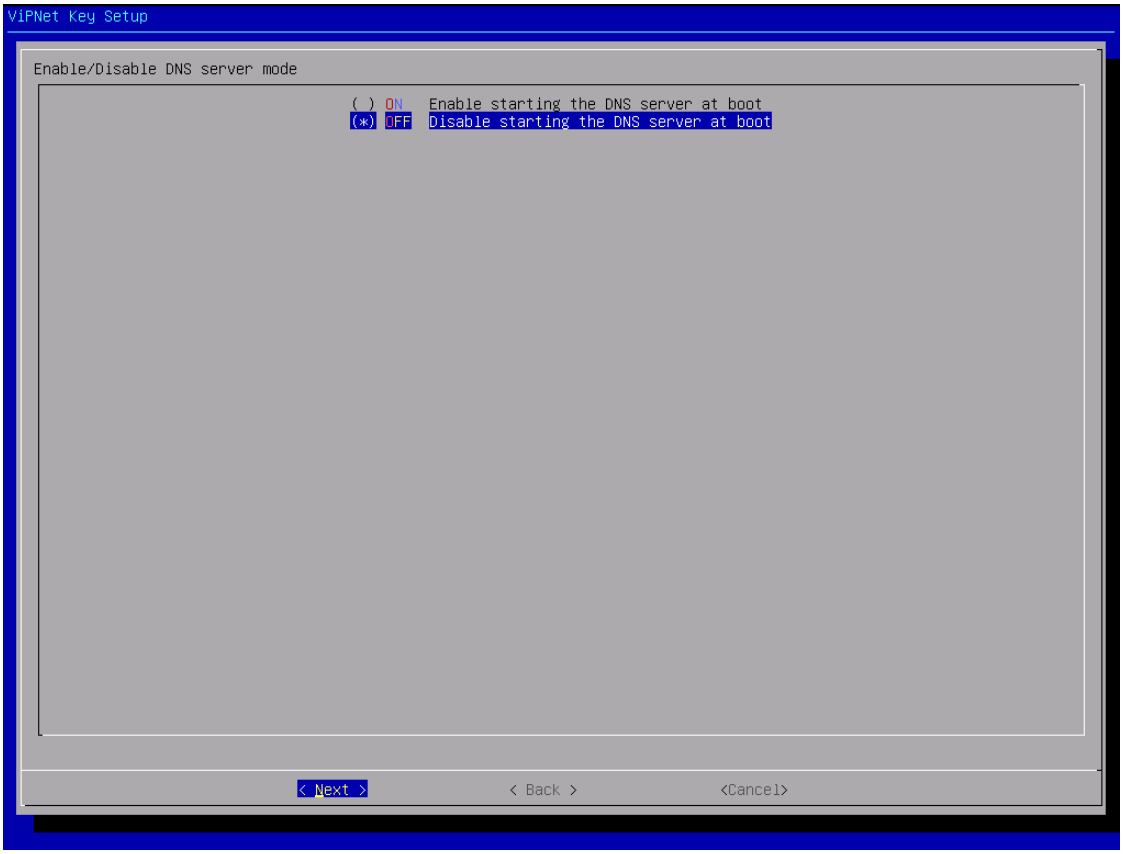

Рисунок 26

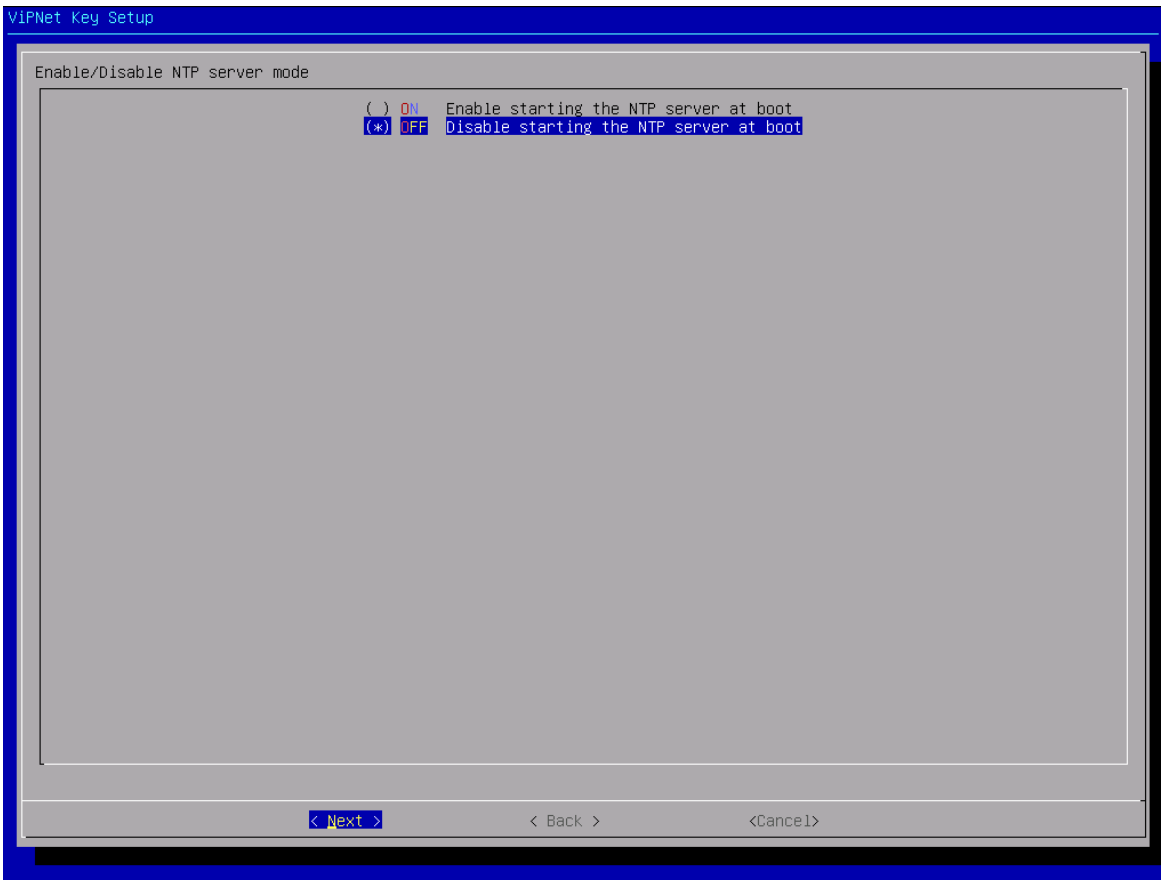
ViPNet Key Setup
Enable/Disable NTP server mode
( ) ON Enable starting the NTP server at boot
(*) OFF Disable starting the NTP server at boot
< Next >
< Back >
<Cancel>

Рисунок 27

Имя координатора должно соответствовать его физическому расположению и принадлежности к той или иной медицинской организации, а так же примерно совпадать с его именем в ЦУС (данное имя можно уточнить у Администратора сети) или посмотреть на название папки с *.dst или “имя”.xps. Если имя в ЦУС не совпадает с физическим местоположением координатора, то сообщите об этом Администратору сети (например координатор переехал из одного филиала в другой).

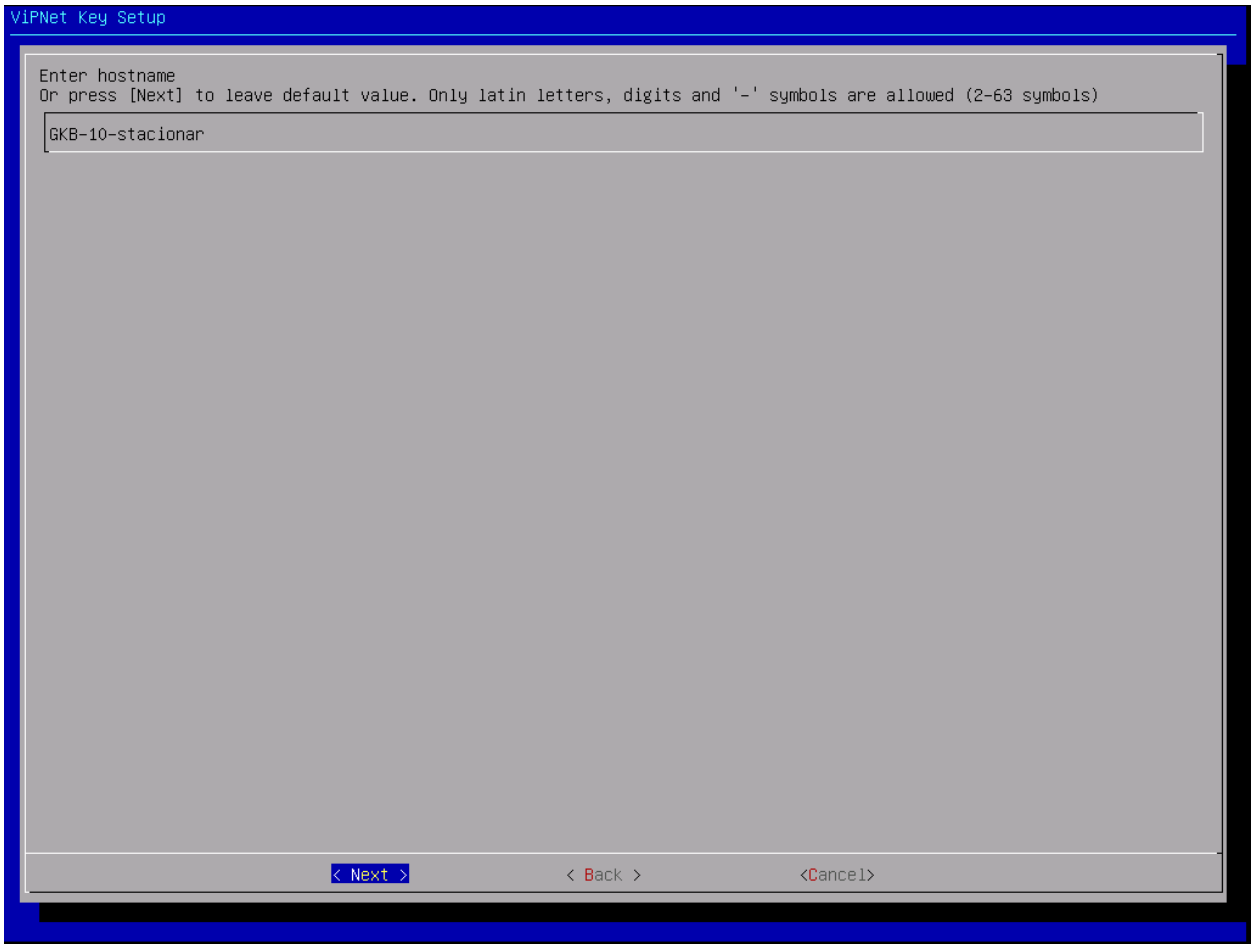

Рисунок 28

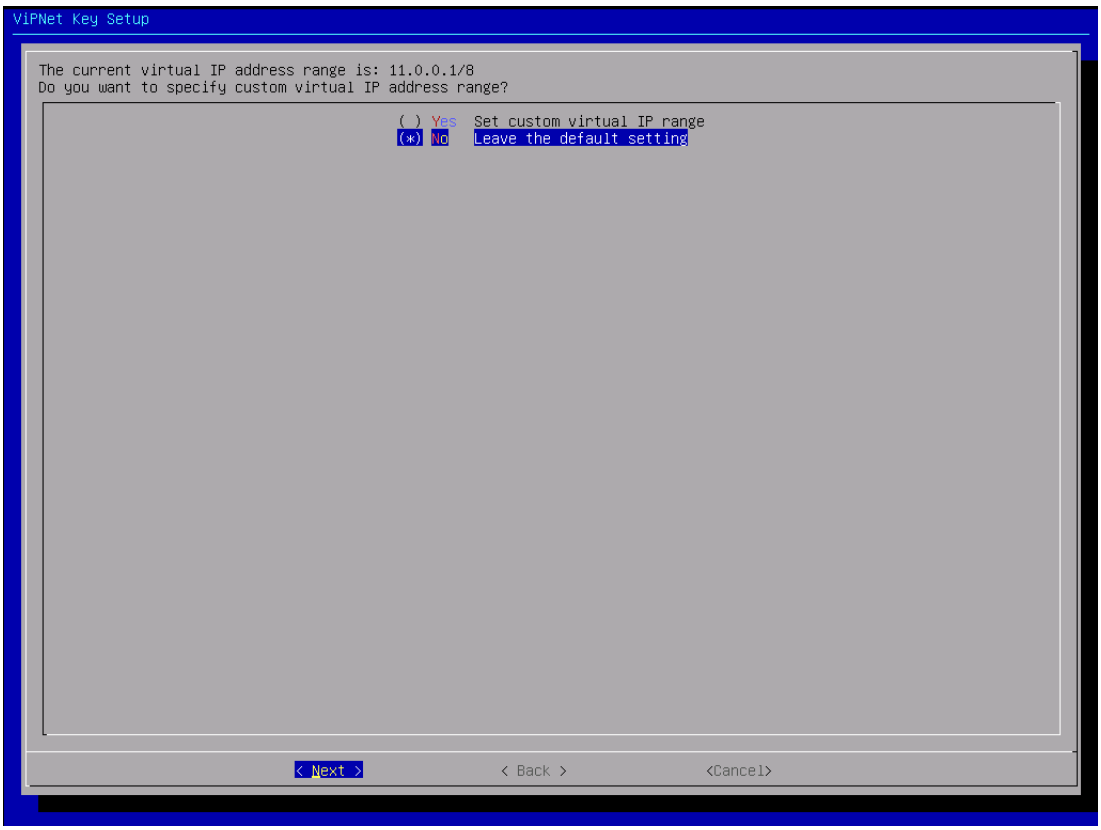

Рисунок 29

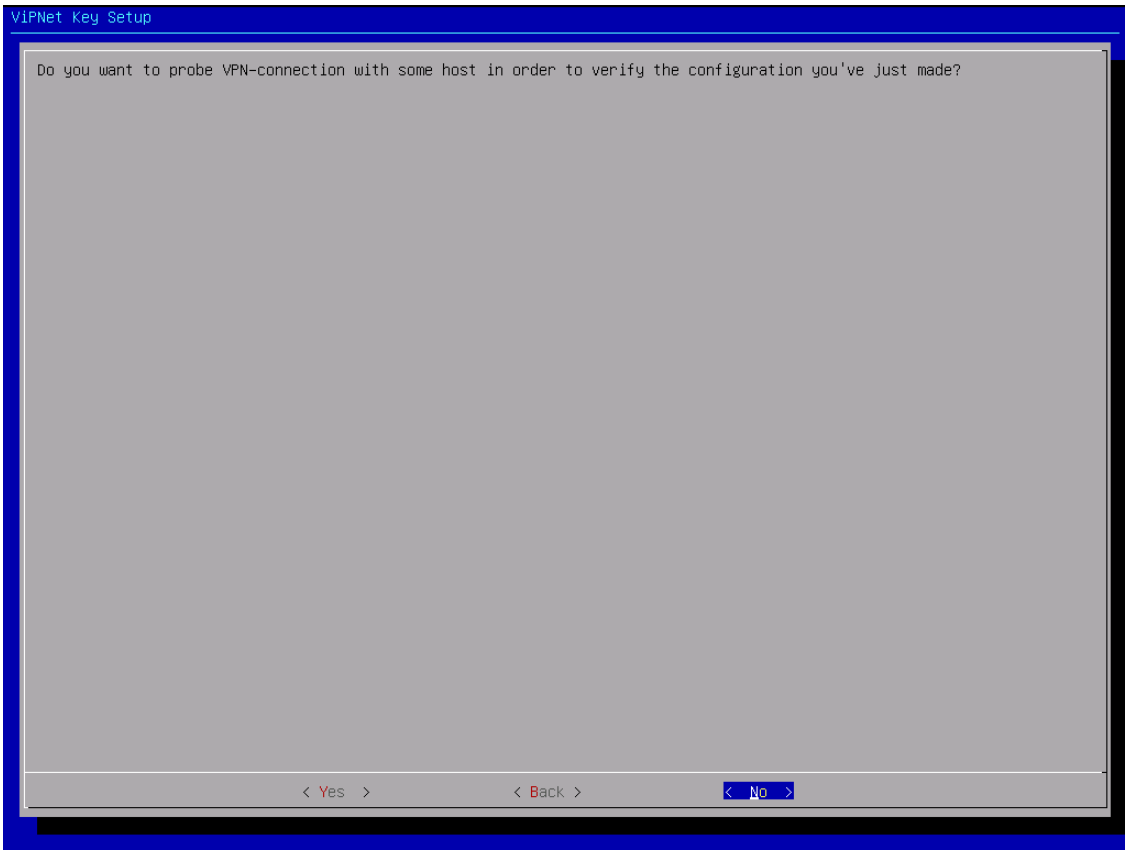

Рисунок 30

Рисунок 31

Finish – начинается перезагрузка.

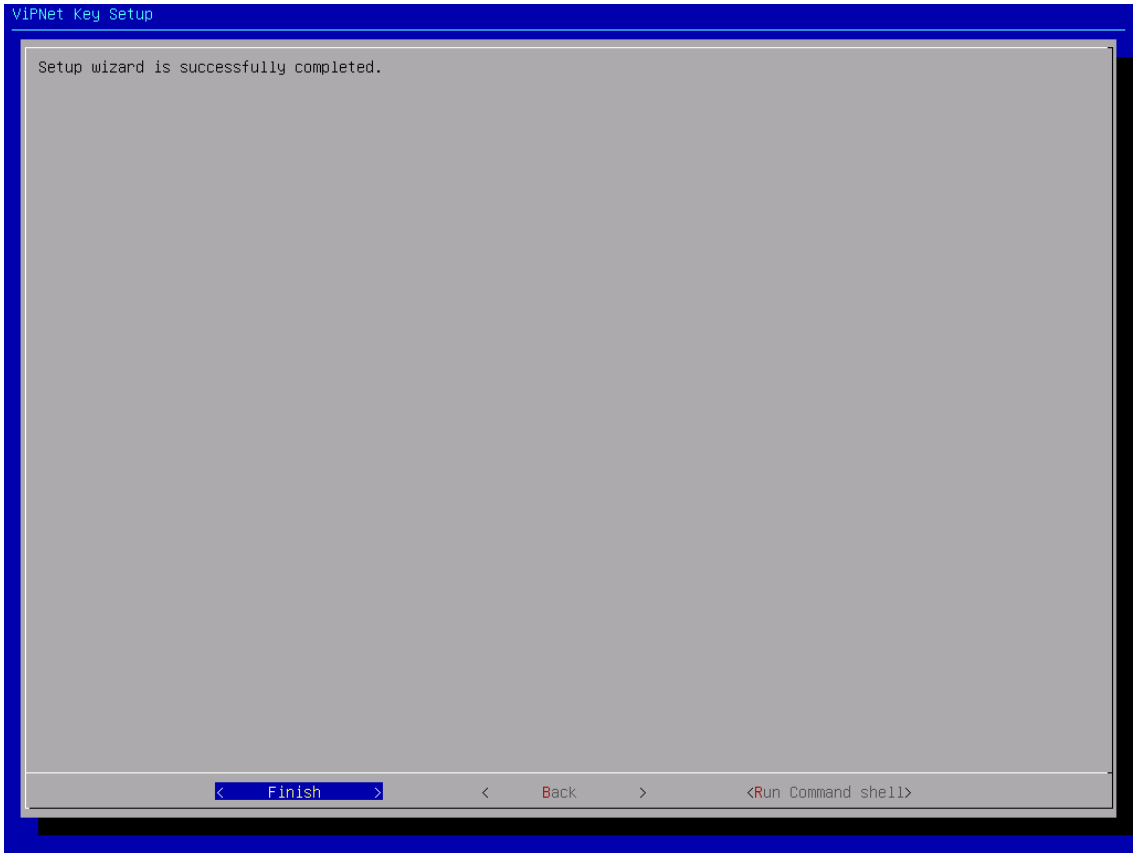

Рисунок 32

После перезагрузки системы, следует настроить конфигурационный файл службы VPN. Для этого необходимо войти в систему с повышенными правами.

Login	user
Password	«в .xps файле»

Рисунок 33

Затем проверяем, правильно ли были настроены сетевые интерфейсы. Обращаем внимание на выделенные места. Красным выделен интерфейс, который и планировалось настроить. Сверьте планируемые настройки с фактическими. Синим выделен интерфейс, который не планировалось включать. Для скроллинга используйте комбинацию клавиш shift + pageUp / shift + pageDown.

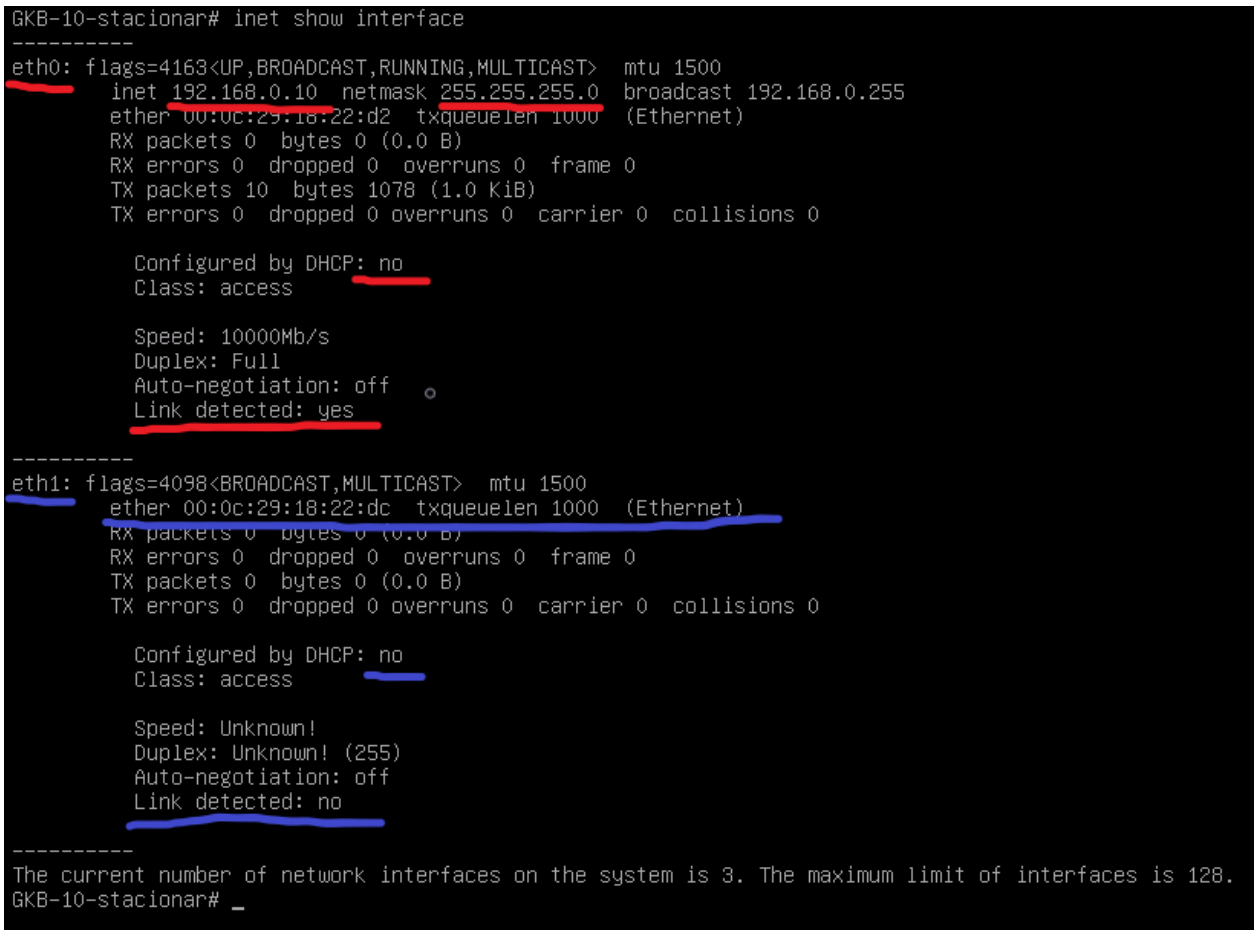

Рисунок 34

Если интерфейсы настроены верно, то можно приступать к настройке конфигурационного файла iplir.conf. Для начала необходимо остановить службу iplir командой *iplir stop*.

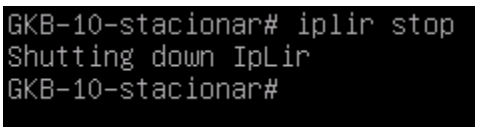

Рисунок 35

Затем открыть конфигурационный файл командой *iplir config*.

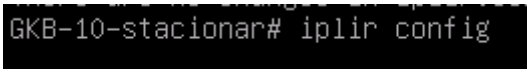

Рисунок 36

Затем необходимо найти в файле секцию [dynamic] (лучше начинать с конца).

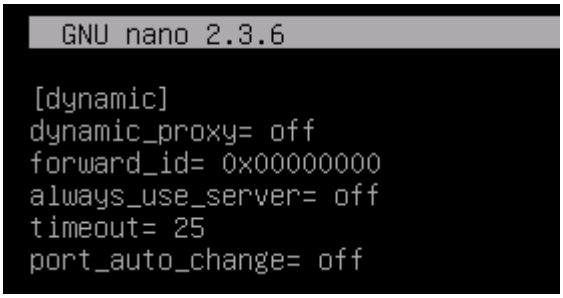

Рисунок 37

Отредактировать в ней следующие параметры:

- dynamic_proxy= on
- forward ID= 0x0c1c2860

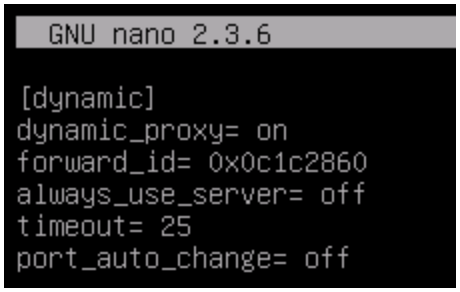

Рисунок 38

После чего сохранить изменения. Для этого комбинацией клавиш *ctrl+x* необходимо выйти из редактора и согласиться с изменениями не изменяя название файла (Enter).

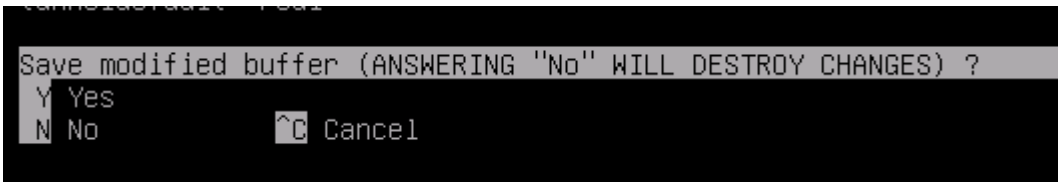

Рисунок 39

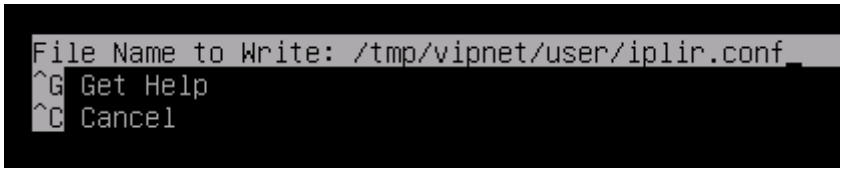

Рисунок 40

После необходимо запустить службу iplir командой *iplir start* и перезагрузить координатор командой *machine reboot*.

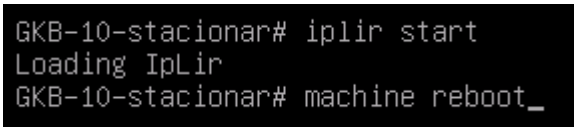

Рисунок 41

Возможные проблемы (FAQ):

1. **Возможна неверная настройка сети.**

Попробуйте проверить сетевую доступность устройства командами:

- *inet ping <ip-address шлюза>*
- *inet ping 8.8.8.8*

Если выполнение данных команд не увенчалось успехом – значит проблема в локальной настройке. Тут Вы сами себе хозяева, помочь не сможем.

2. **Возможно неверно настроен туннель на координаторе или статический маршрут**

Проверьте, есть ли доступ с координатора до ПроМед командами:

- *iplir ping 0x0c1c2860* (если команда считается неправильной введите iplir start и повторите)
- *iplir ping* 10.62.15.30

Если команды завершились успешно – значит проблема или в туннеле или в маршруте – подсказа по настройке маршрута есть на *сайте миац-рб.рф → Деятельность → Информационная безопасность*.

3. **Проверка настроек туннеля**

Введите команду *iplir show config* . В первой секции [id] будут указаны туннели, которые заданы Вашему координатору. Для их смены необходимо написать заявку на почту oib@doctorrb.ru и указать в нем название координатора и требуемое адресное пространство для туннелирования.

4. **Проверка настроек конфигурационного файла**

Введите команду iplir show config и в случае, когда корд стоит сбоку (один активный сетевой интерфейс) проверьте следующие параметры:

- В собственной секции [id] (самая первая где ваши туннели): о параметр usefirewall установите в значение on;
- В секции [dynamic]: о параметр dynamic_proxy установите в значение on;
- в параметре forward_id = 0x0c1c2860;

5. **Для предоставление удаленного доступа по ssh**

firewall local add src (айпишник с которого будешь заходить) dst (айпишник корда) service @SSH pass

6. **Telegram чат для решения и обсуждения проблем**

https://t.me/+QSyMCxV085szMjVi