S-CRYPTO VPN 1.0

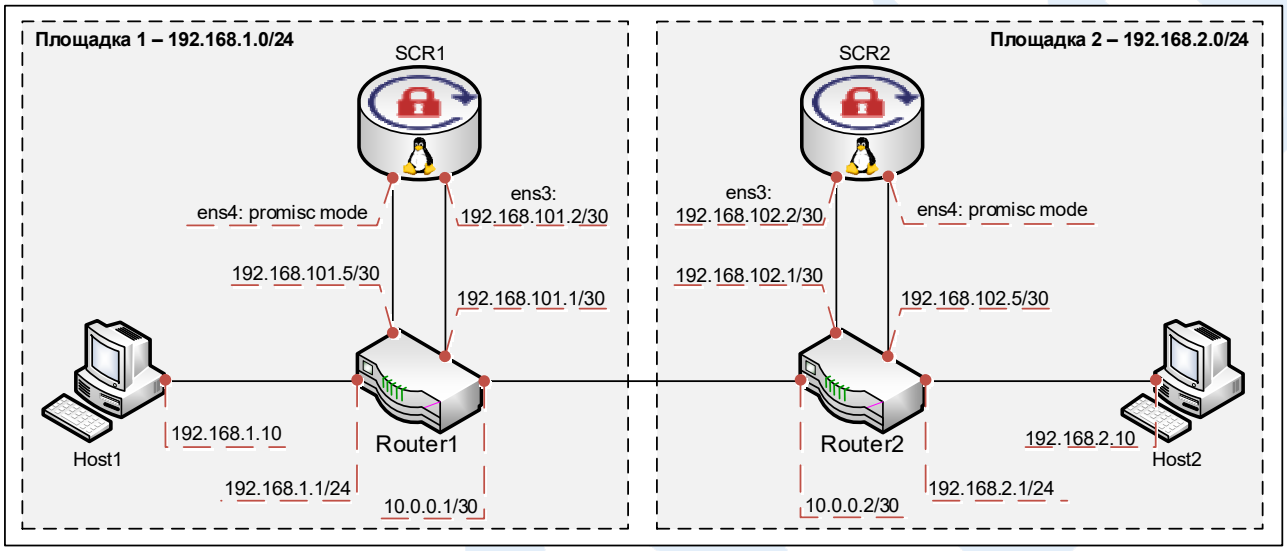
Соединение между площадками (Site-to-Site). Построение туннеля между двумя шлюзами «S-Crypto VPN Server» на ОС Debian с маршрутизацией между защищаемыми сегментами встроенным виртуальным маршрутизатором

Оглавление

1. **Описание стенда** 2
2. **Логика работы** 2
3. **Описание устройства «Host1»** 3
4. **Описание устройства «Host2»** 3
5. **Описание устройства «Router1»** 3
6. **Описание устройства «Router2»** 4
7. **Настройка шлюза безопасности «SCR1»** 4
8. **Настройка шлюза безопасности «SCR2»** 9
9. **Проверка работоспособности стенда** 17

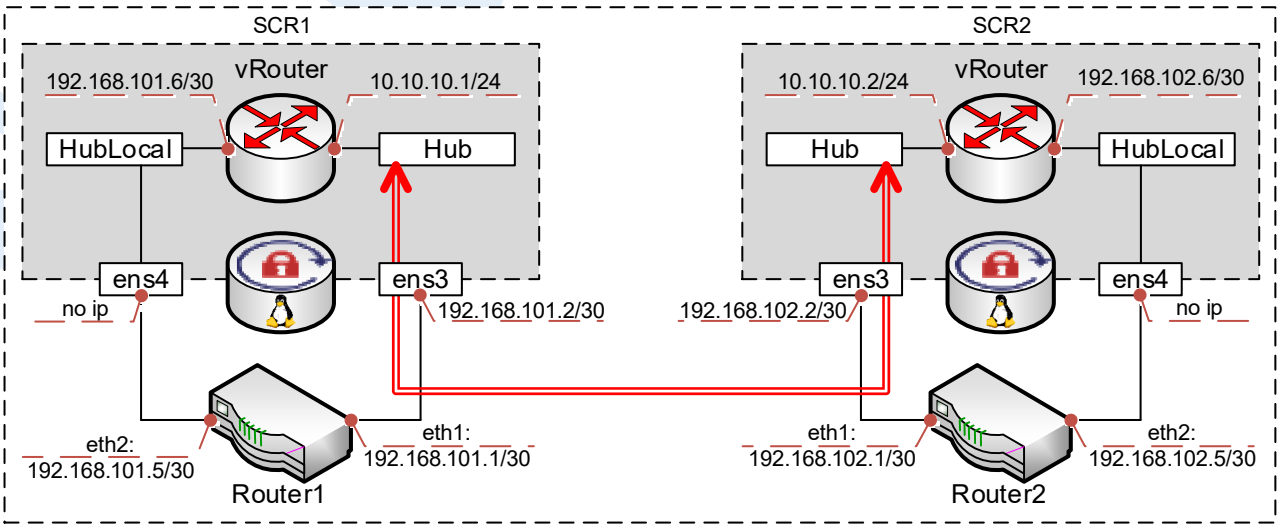
1. Описание стенда

Сценарий содержит пример настройки шлюзов безопасности «S-Crypto VPN Server», установленных на операционной системе Debian, с целью безопасного межсетевого взаимодействия между двумя удаленными площадками. Взаимодействие между устройствами в локальных сетях осуществляется путем маршрутизации трафика средствами встроенного виртуального маршрутизатора шлюзов безопасности «SCR1» и «SCR2».



2. Логика работы

На каждом из шлюзов безопасности «SCR1» и «SCR2» будет создан виртуальный хаб «Hub», для создания безопасного туннельного соединения между ними, и виртуальный хаб «HubLocal» для взаимодействия с локальной сетью своей площадки. Маршрутизация между сегментами (хабами) будет осуществляться с помощью функции виртуального маршрутизатора.



Шлюзы безопасности «SCR1» и «SCR2» подключены двумя интерфейсами в центральные маршрутизаторы своих площадок. Маршрутизаторы «Router1» и

«Router2» через интерфейс «eth2» с помощью статических маршрутов направляют трафик, подлежащий шифрованию, на виртуальный хаб «HubLocal» через сетевой интерфейс «ens4», находящийся в неразборчивом режиме, шлюза безопасности своей площадки. Затем с помощью виртуального маршрутизатора трафик поступает на виртуальный хаб «Hub» и после шифрования инкапсулированный трафик через интерфейс «ens3» возвращается на маршрутизатор, с которого направляется в адрес соседней площадки, где в обратной последовательности производится его расшифровка.

3. Описание устройства «Host1»

Устройство с операционной системой Windows 7 с назначенным статическим ip-адресом 192.168.1.10/24 gw 192.168.1.1 и установленным программным продуктом «S-Crypto VPN Server Manager» для возможности удаленного администрирования шлюзов безопасности «SCR1» и «SCR2» с помощью графического пользовательского интерфейса. Также используется в сценарии для проверки защищенного межсетевого взаимодействия.

4. Описание устройства «Host2»

Устройство с операционной системой Windows 7 с назначенным статическим ip-адресом 192.168.2.10/24 gw 192.168.2.1 и установленным программным продуктом «S-Crypto VPN Server Manager» для возможности удаленного администрирования (первичной настройки) шлюза безопасности «SCR2» с помощью графического пользовательского интерфейса. Также используется в сценарии для проверки защищенного межсетевого взаимодействия.

5. Описание устройства «Router1»

«Router1» – маршрутизатор, с назначенными статическими ip-адресами в соответствии со схемой в разделе 1, и обеспечивающий следующие функции:

1. Доступ устройств, находящихся в локальной сети «Площадка 1», в неконтролируемый сегмент (Интернет);

2. Проброс (DNAT) TCP-порта, в приведенном сценарии TCP:1355, с внешнего интерфейса маршрутизатора 10.0.0.1 на сетевой интерфейс ens3:192.168.101.2 шлюза безопасности «SCR1».

На устройстве добавлены два статических маршрута для направления трафика, подлежащего шифрованию, на виртуальный маршрутизатор шлюза безопасности «SCR1»:

– 192.168.2.0/24 via 192.168.101.6 – для взаимодействия между

устройствами в локальных сетях площадок через защищенное соединение;

– 192.168.102.2/32 via 192.168.101.6 – для удаленного администрирования шлюза безопасности «SCR2» с устройства «Host1».

6. Описание устройства «Router2»

Устройство «Router2» – маршрутизатор, обеспечивающий доступ устройств, находящихся сети «Площадки 2», в неконтролируемый сегмент (Интернет). На сетевых интерфейсах устройства назначены статические ip-адреса в соответствии со схемой в разделе 1. Добавлен статический маршрут: 192.168.1.0/24 via 192.168.102.6

7. Настройка шлюза безопасности «SCR1»

Шлюз безопасности «SCR1» – устройство на базе операционной системы Debian с установленным продуктом «S-Crypto VPN Server».

1. Настройте сетевые интерфейсы. Пример файла /etc/network/interfaces:

```
auto lo
iface lo inet loopback

allow-hotplug ens3
iface ens3 inet static
address 192.168.101.2
netmask 255.255.255.252
gateway 192.168.101.1

allow-hotplug ens4
iface ens4 inet manual
```

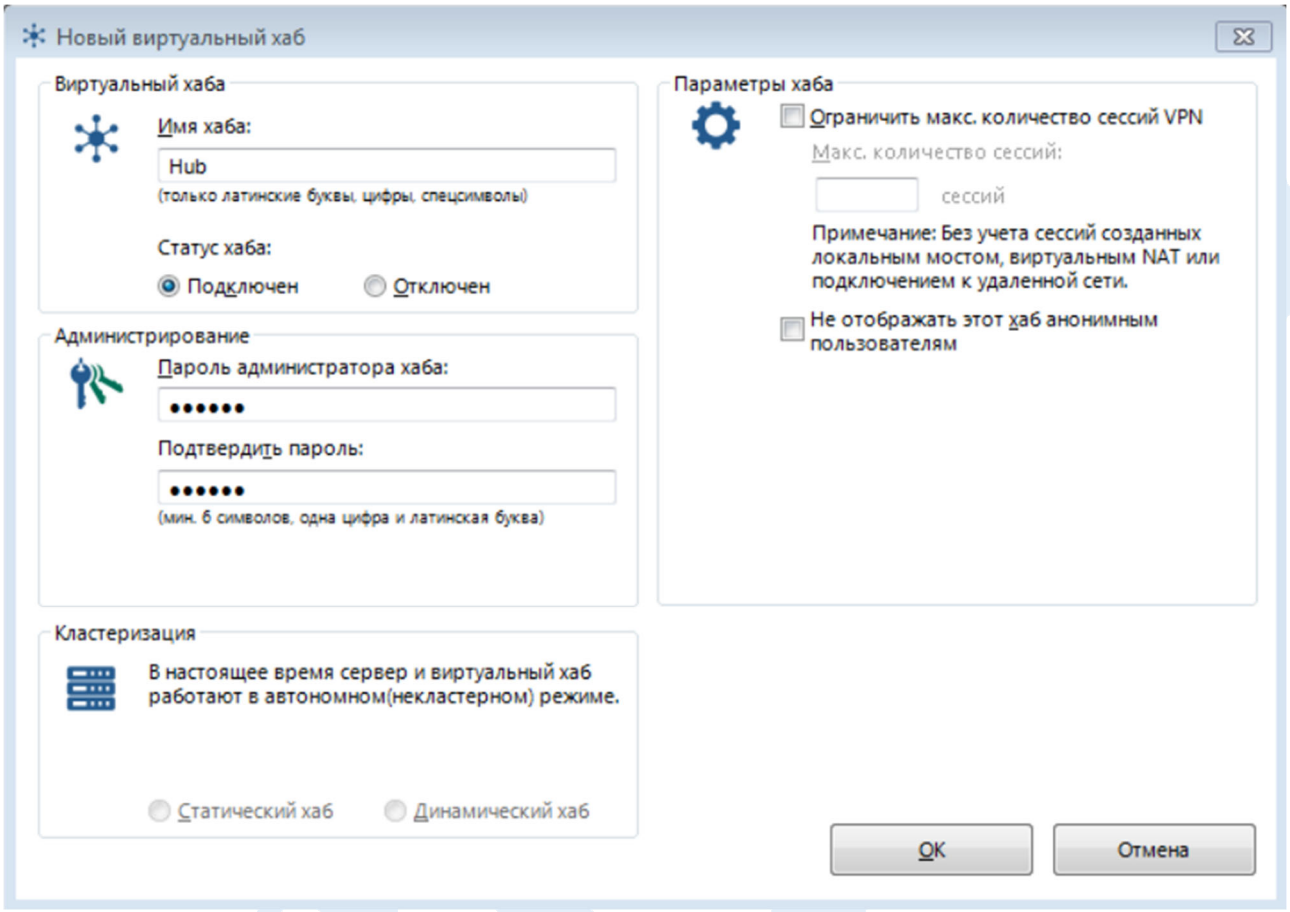
После внесения изменений перезапустите сетевую службу командой `sudo systemctl restart networking`

На интерфейсе «ens3» назначен статический ip-адрес, на котором прослушивается порт TCP:1355 для терминирования входящих подключений от шлюза «SCR2». Интерфейс «ens4» не имеет ip-адреса и будет переведён в неразборчивый режим (promiscuous mode).

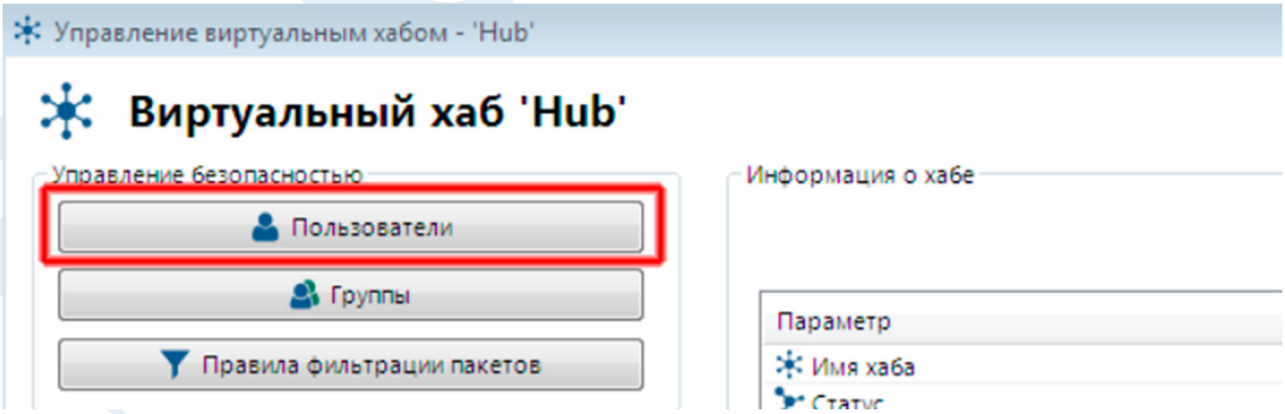
2. Установите программное обеспечение «S-Crypto VPN Server» в соответствии с инструкцией «Руководство администратора».

3. Дальнейшую настройку производите с устройства «Host1», предварительно настроив подключение программы «S-Crypto VPN Server Manager» к устройству «SCR1» и введя информацию о лицензии для запуска сервера, в соответствии с инструкцией «Руководство администратора» доступной в комплекте поставки, а также на официальном сайте компании в разделе «Техническая поддержка» - «Документация» https://s-crypto.by/support-pages/documentation/.

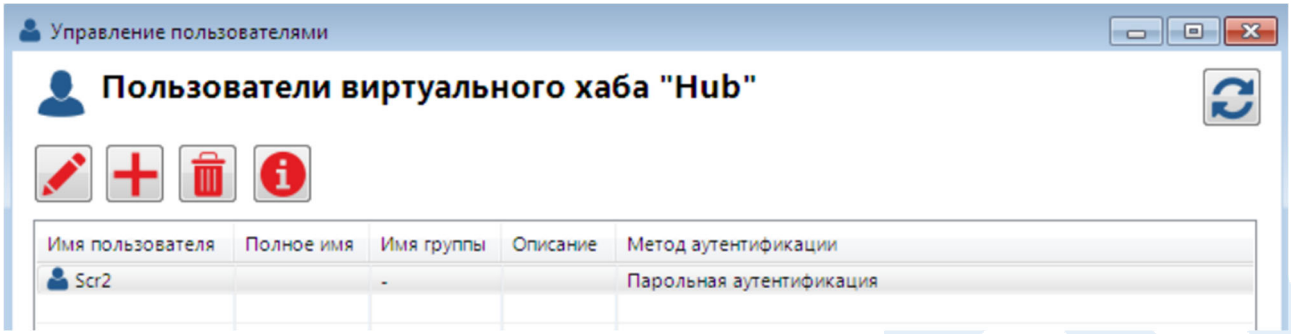
4. С устройства «Host1» с помощью программы «S-Crypto VPN Server Manager» подключитесь к серверу «SCR1» по адресу 192.168.101.2 и создайте, если ещё не создан, виртуальный хаб «Hub» для терминирования входящих подключений



5. В настройках созданного виртуального хаба «Hub» откройте раздел «Пользователи»

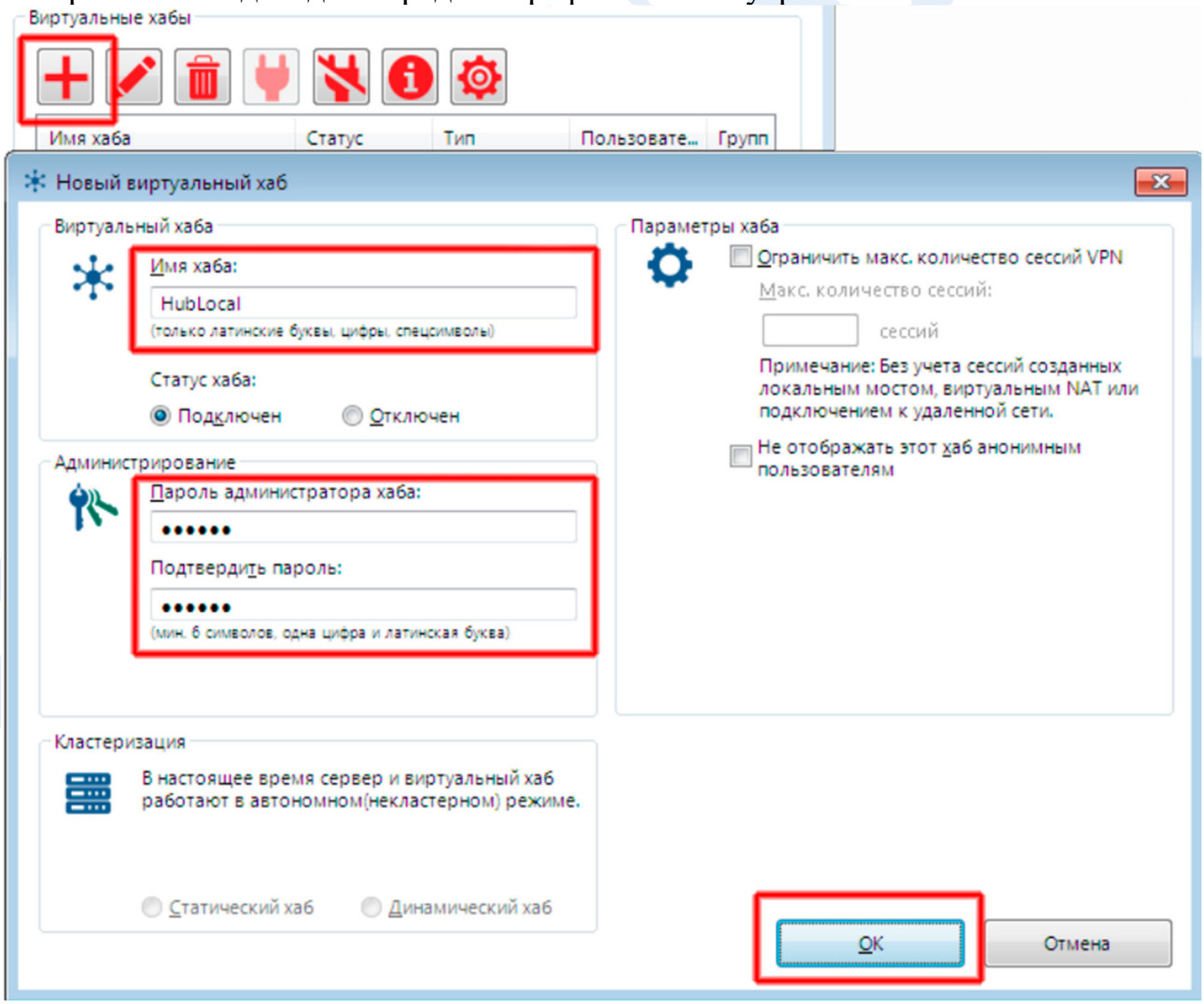


6. Создайте учетную запись, от имени которой будет аутентифицироваться подключение со стороны сервера «SCR2»

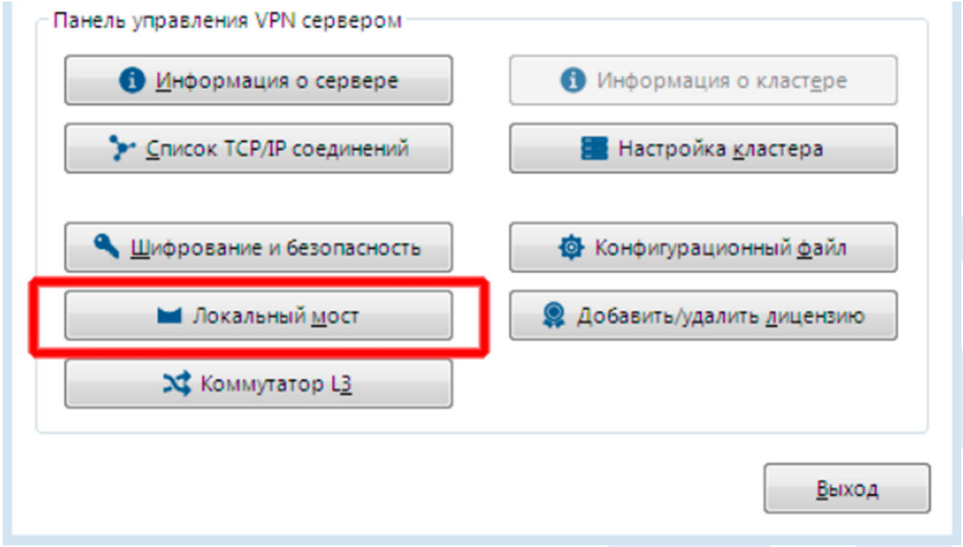


Информация о настройке различных способов аутентификации пользователей размещена в инструкции «Способы аутентификации» доступной на официальном сайте компании в разделе «Техническая поддержка» - «Документация» https://s-crypto.by/support-pages/documentation/

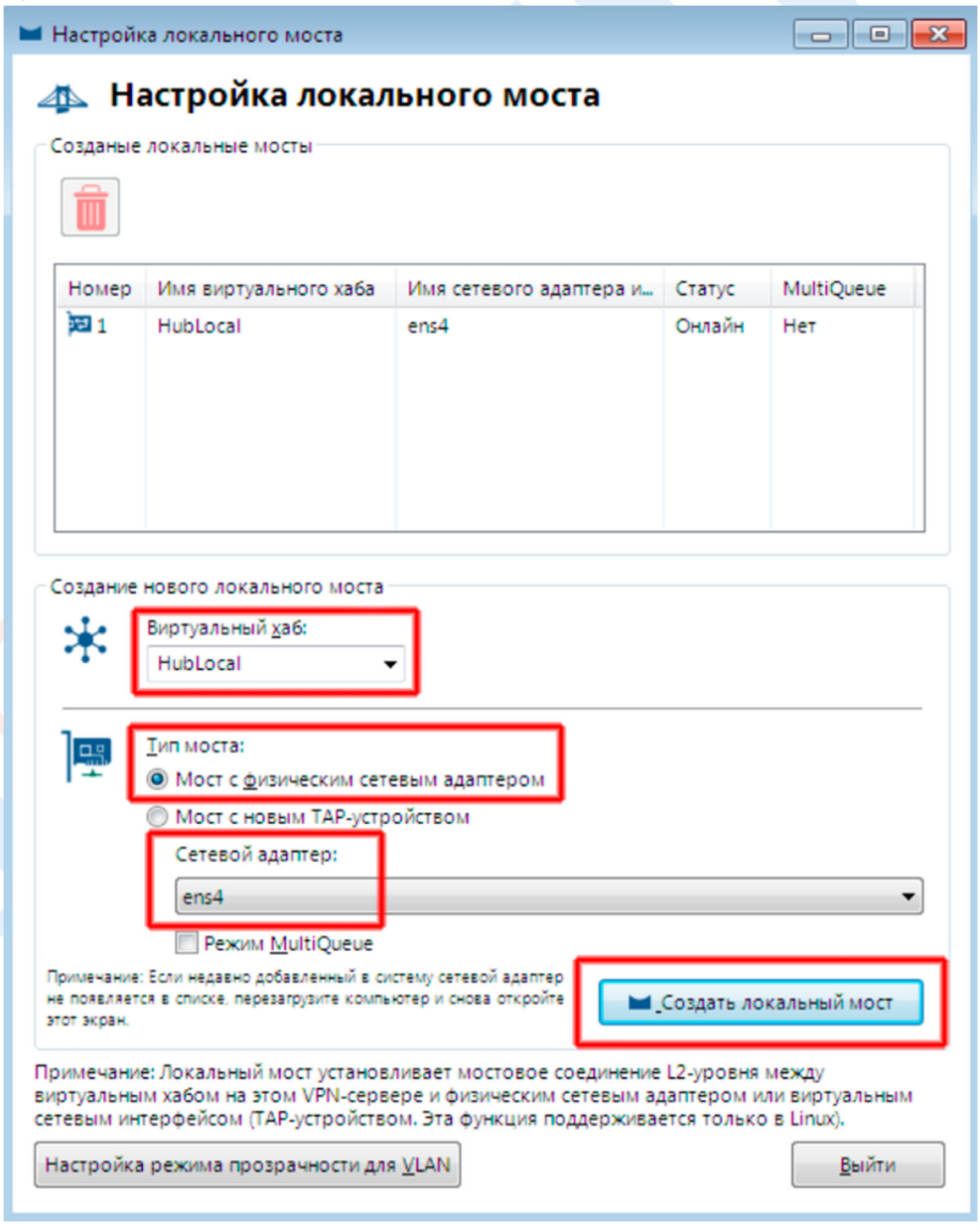
7. В настройках сервера создайте новый виртуальный хаб «HubLocal», который необходим для передачи трафика в/из внутреннего сегмента



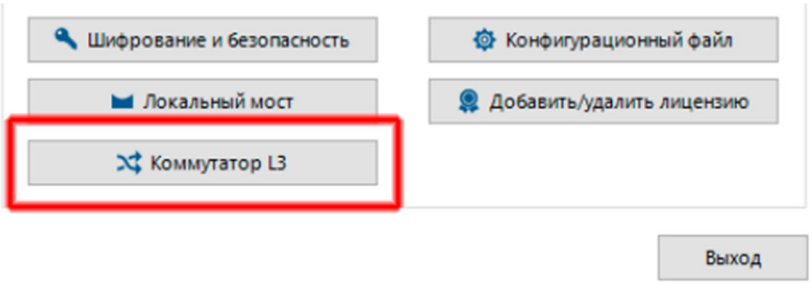
8. В настройках сервера зайдите в раздел «Локальный мост»



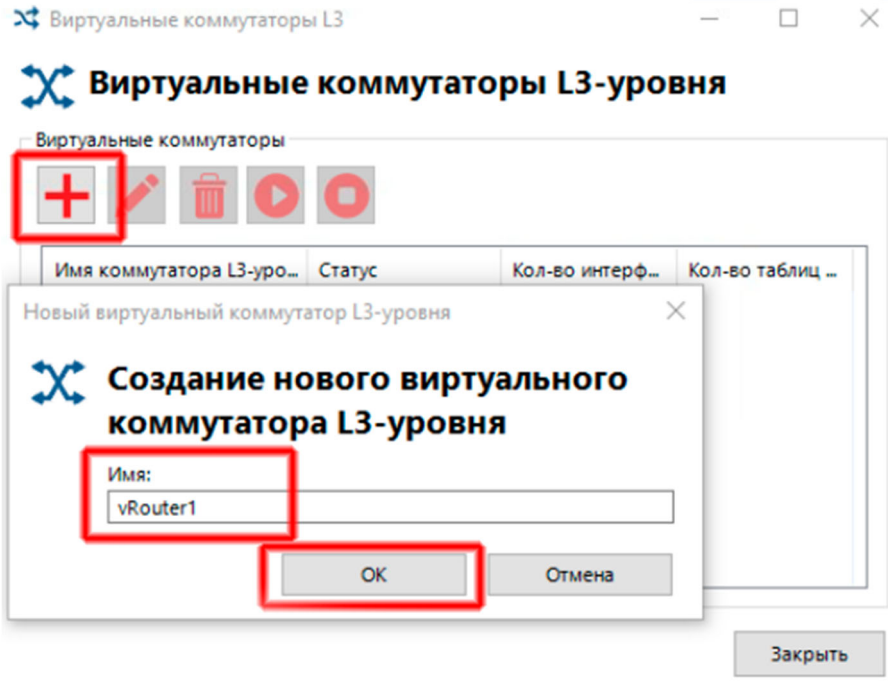
9. Создайте локальный мост от виртуального хаба «HubLocal» к сетевому интерфейсу «ens4»



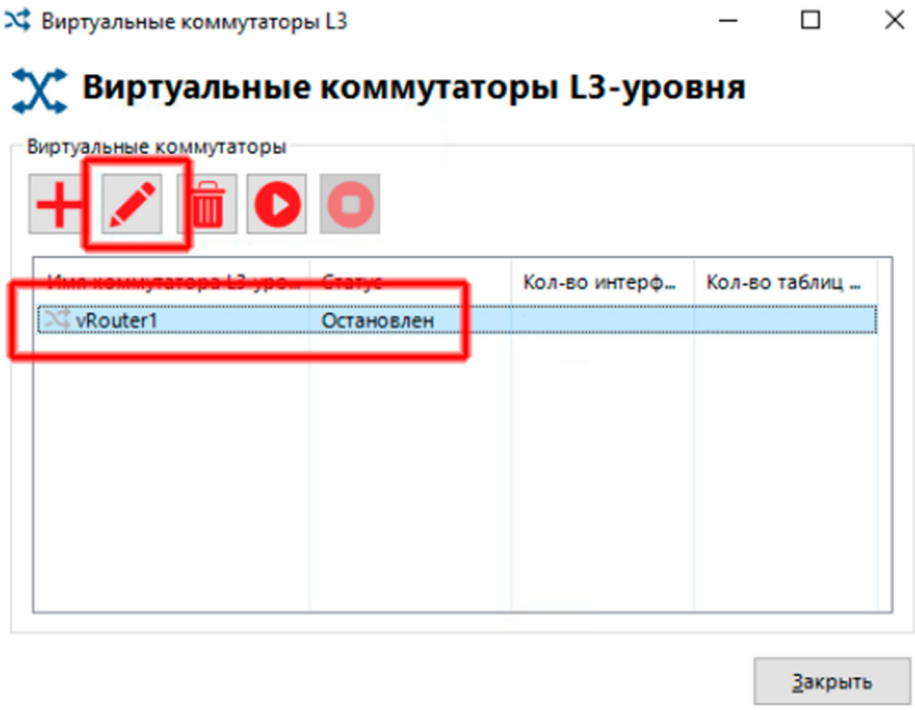
10. В настройках сервера зайдите в раздел «Коммутатор L3»



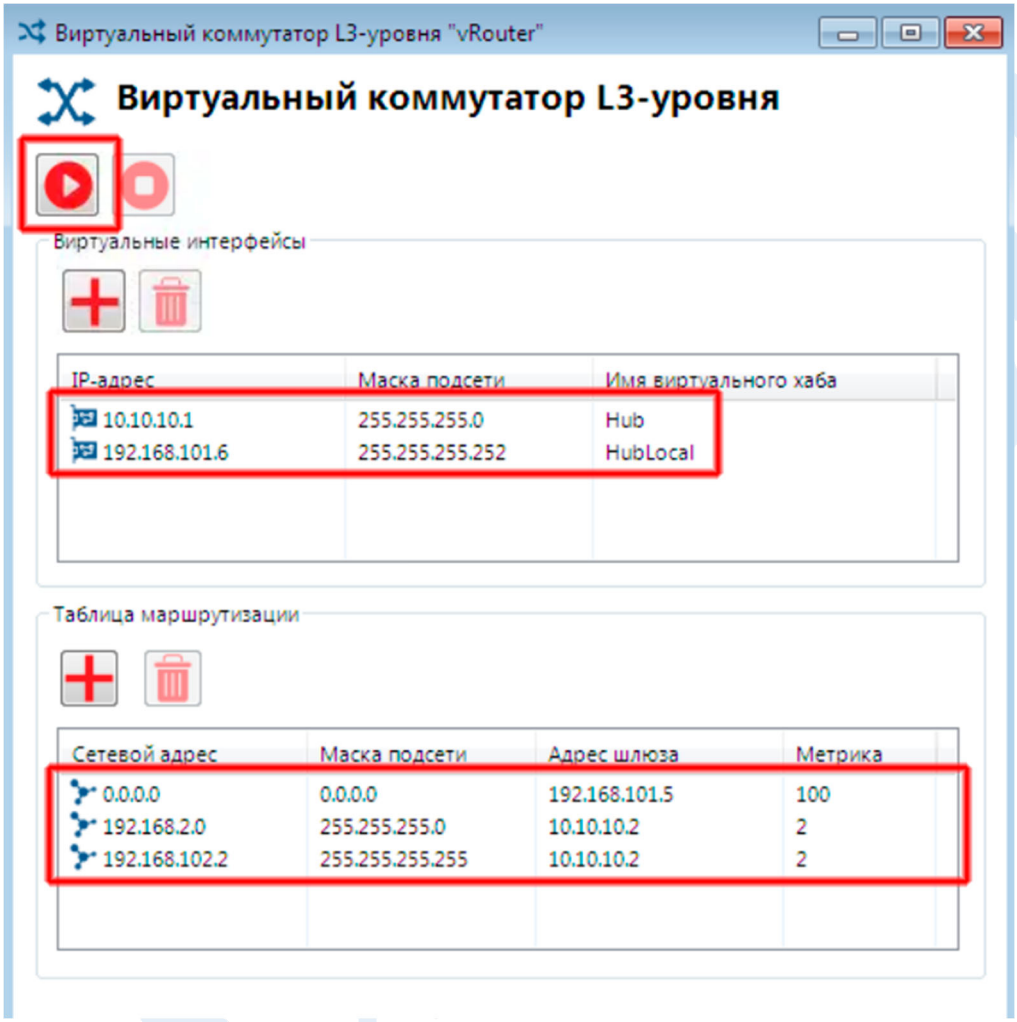
11. Нажмите «Добавить новый коммутатор», введите его имя и затем нажмите «ОК».



12. Зайдите в настройки созданного виртуального маршрутизатора



13. Настройте виртуальный маршрутизатор задав ip-адреса для каждого виртуального хаба, адрес шлюза по-умолчанию, маршрут ко второй площадке и маршрут для удаленного администрирования шлюза безопасности «SCR2». Затем включите виртуальный маршрутизатор нажатием кнопки «Активировать».



8. Настройка шлюза безопасности «SCR2»

Шлюз безопасности «SCR2» – устройство на базе операционной системы Debian с установленным продуктом «S-Crypto VPN Server».

1. Настройте сетевые интерфейсы. Пример файла /etc/network/interfaces:

```
auto lo
iface lo inet loopback

allow-hotplug ens3
iface ens3 inet static
address 192.168.102.2
netmask 255.255.255.252
gateway 192.168.102.1

allow-hotplug ens4
iface ens4 inet manual
```

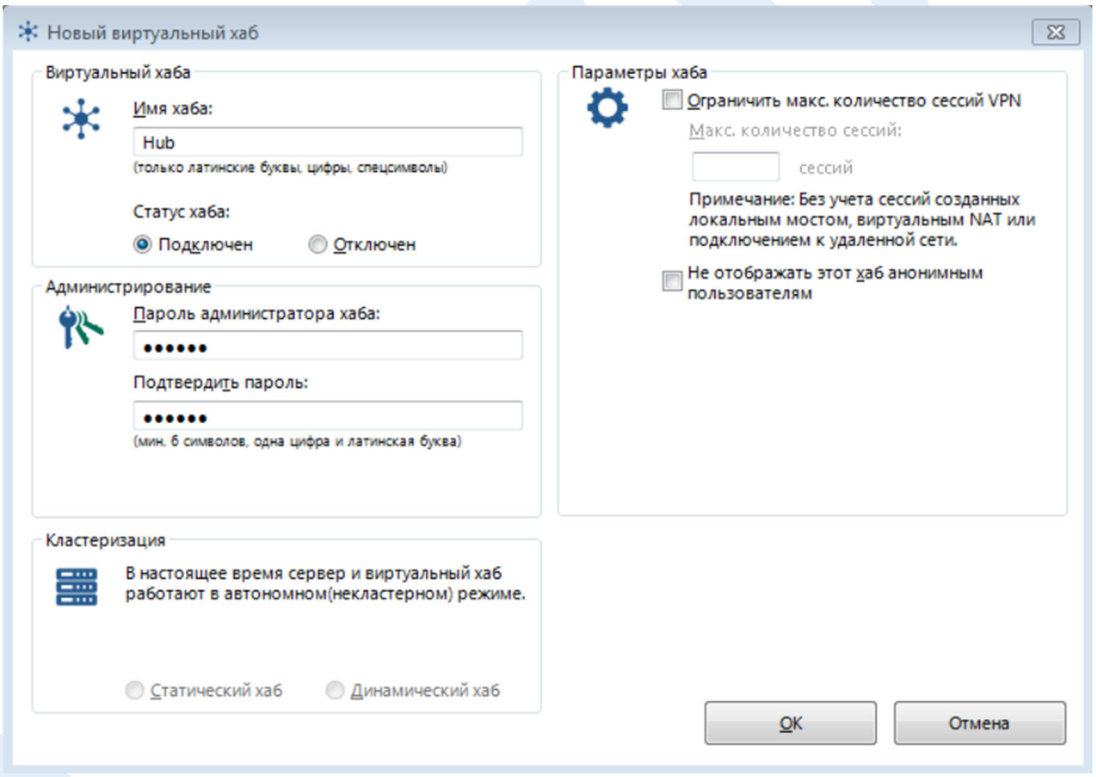
После внесения изменений перезапустите сетевую службу командой `sudo systemctl restart networking`

На интерфейсе «ens3» назначен статический ip-адрес, интерфейс «ens4» не имеет ip-адреса и будет переведён в неразборчивый режим (promiscuous mode).

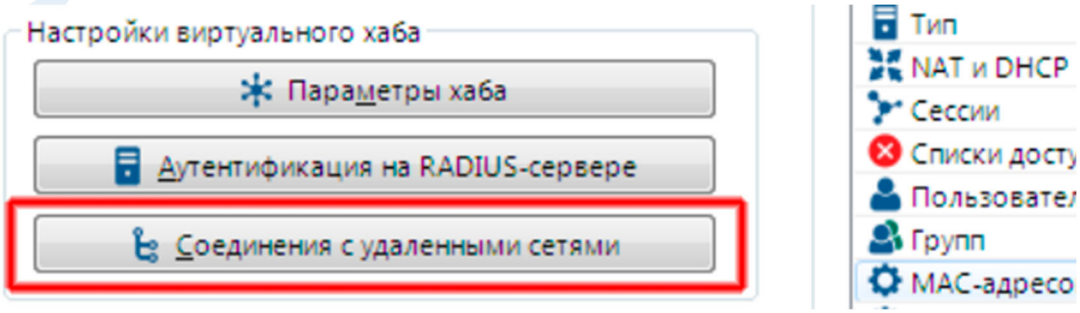
2. Установите программное обеспечение «S-Crypto VPN Server» в соответствии с инструкцией «Руководство администратора».

3. Дальнейшую настройку производите с устройства «Host2», предварительно настроив подключение программы «S-Crypto VPN Server Manager» к устройству «SCR2» и введя информацию о лицензии для запуска сервера, в соответствии с инструкцией «Руководство администратора» доступной в комплекте поставки, а также на официальном сайте компании в разделе «Техническая поддержка» - «Документация» https://s-crypto.by/support-pages/documentation/.

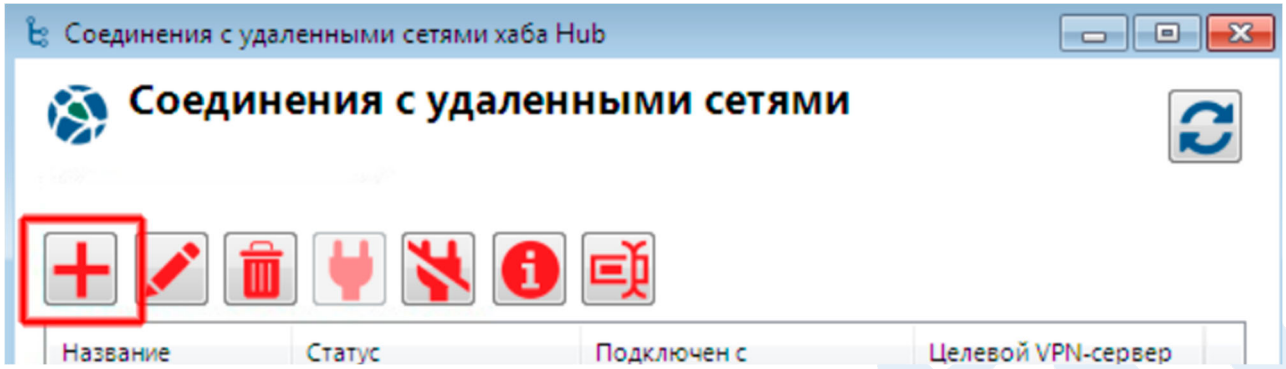
4. С устройства «Host2» с помощью программы «S-Crypto VPN Server Manager» подключитесь к серверу «SCR2» по адресу 192.168.102.2 и создайте, если ещё не создан, виртуальный хаб «Hub» с которого будет инициировано подключение к шлюзу «SCR1»



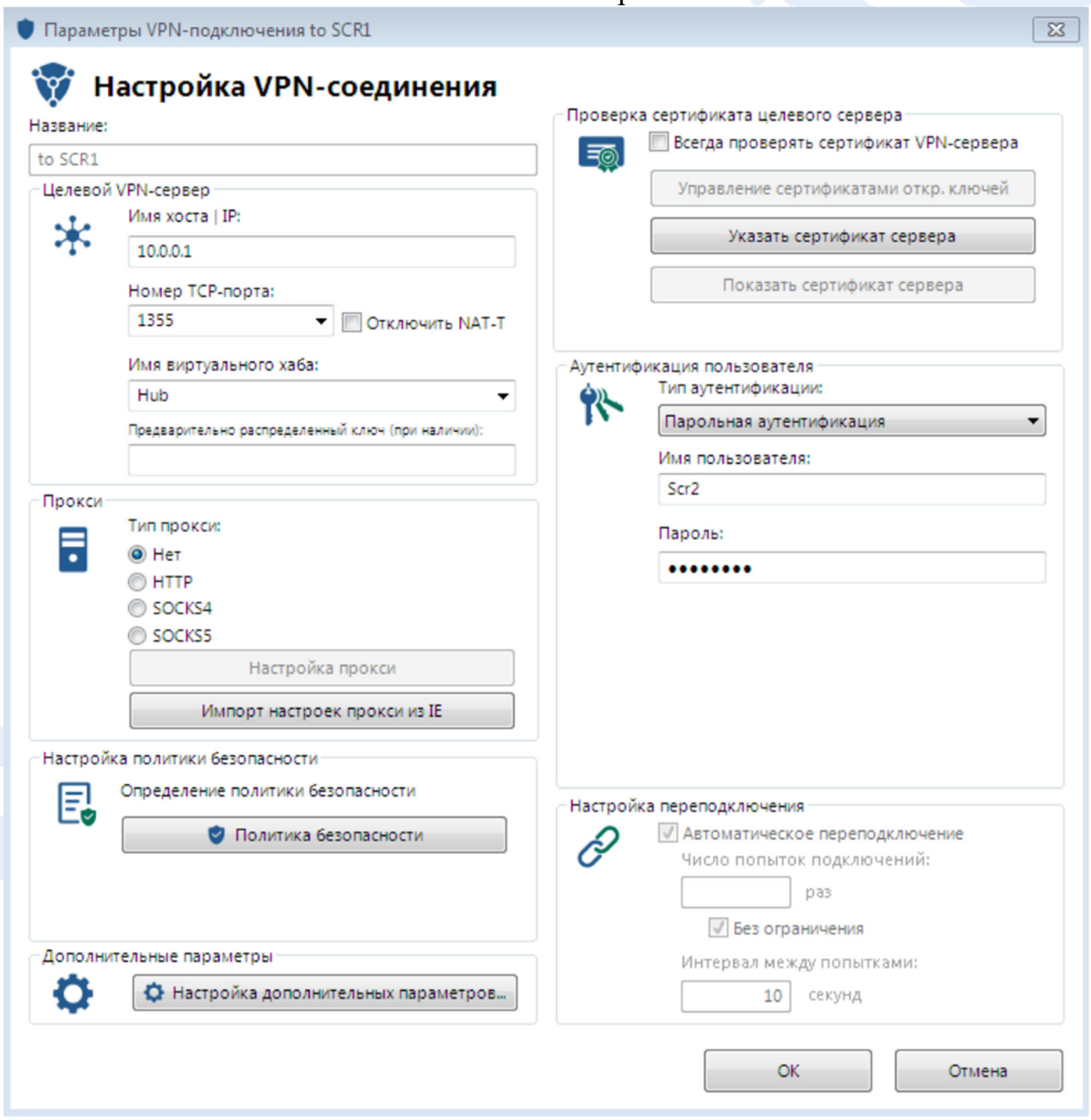
5. В настройках созданного виртуального хаба «Hub» откройте раздел «Соединения с удаленными сетями»



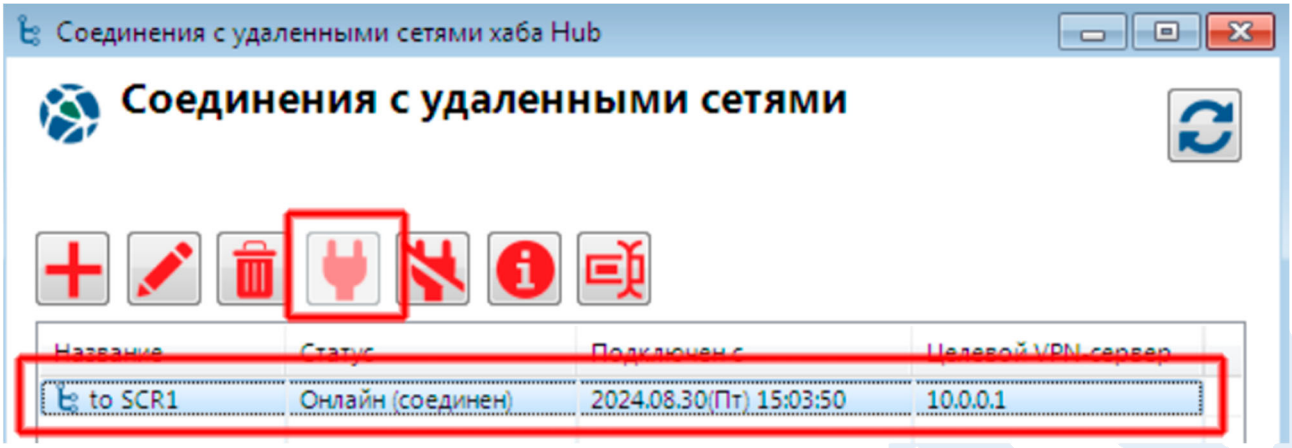
6. В открывшемся окне нажмите «Добавить соединение»



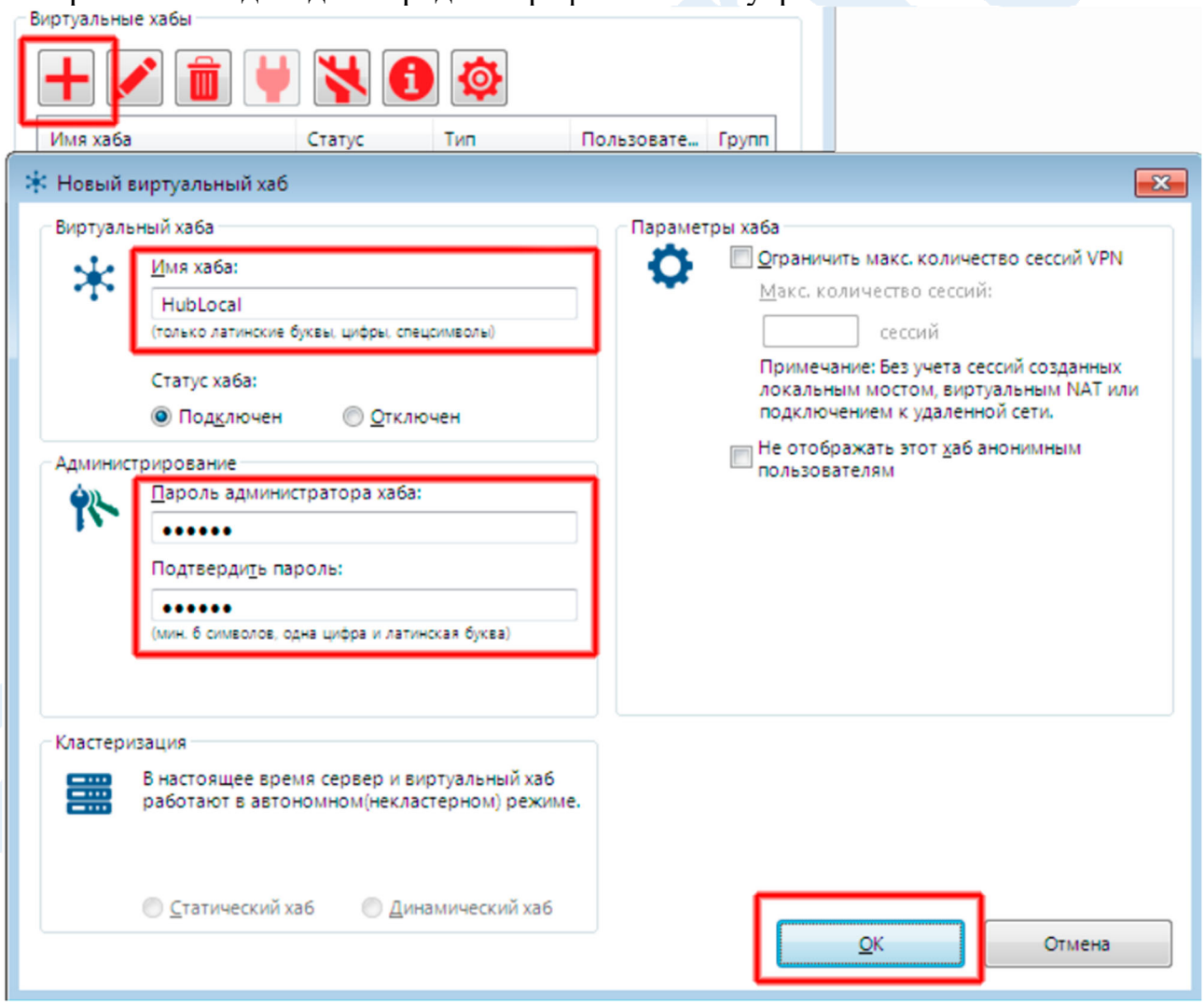
7. Заполните поля в соответствии со скриншотом



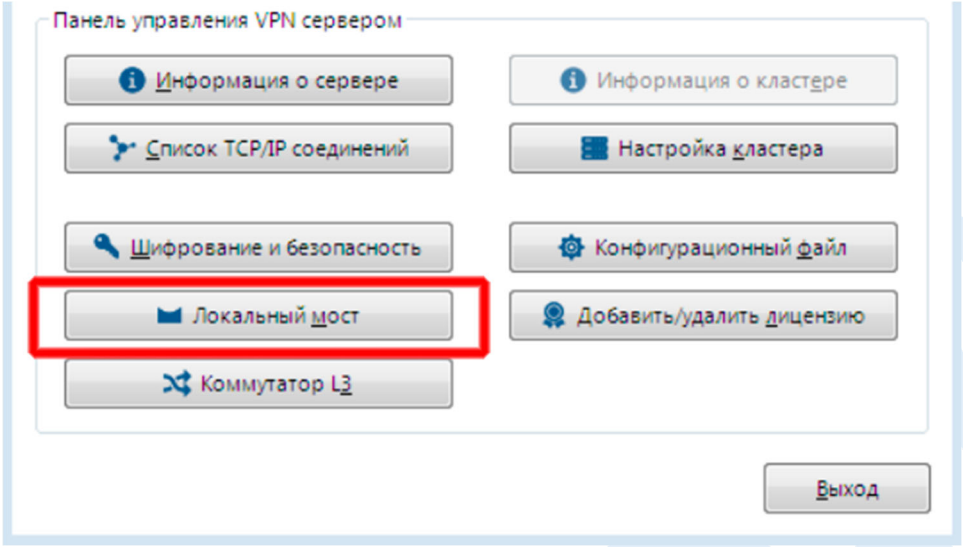
8. После нажатия кнопки «ОК» активируйте созданное подключение



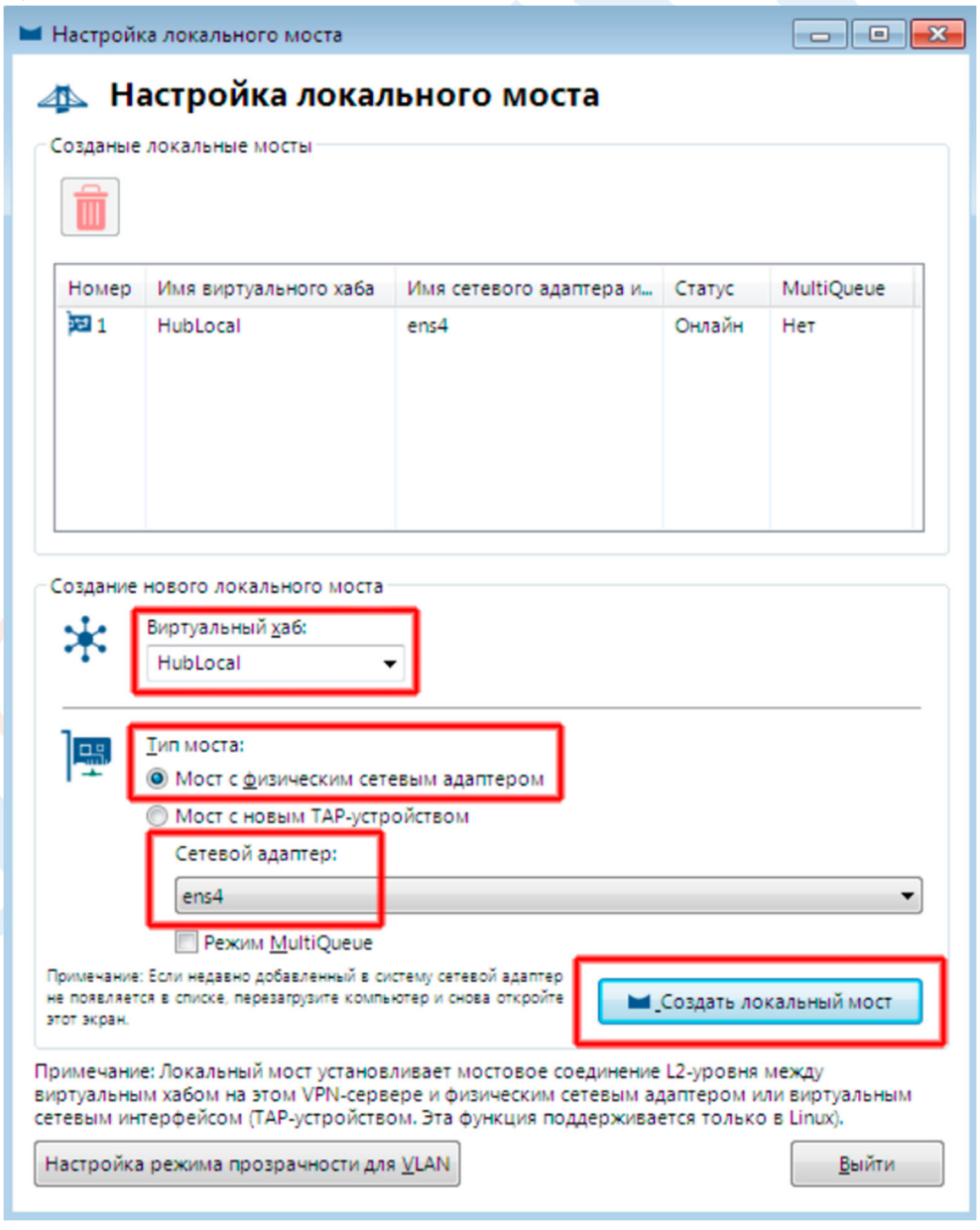
9. В настройках сервера создайте новый виртуальный хаб «HubLocal», который необходим для передачи трафика в/из внутреннего сегмента



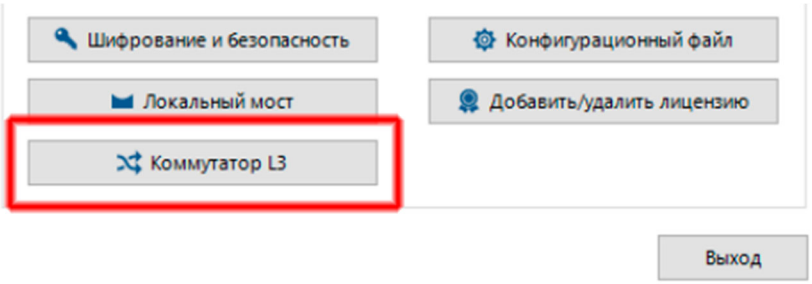
10. В настройках сервера зайдите в раздел «Локальный мост»



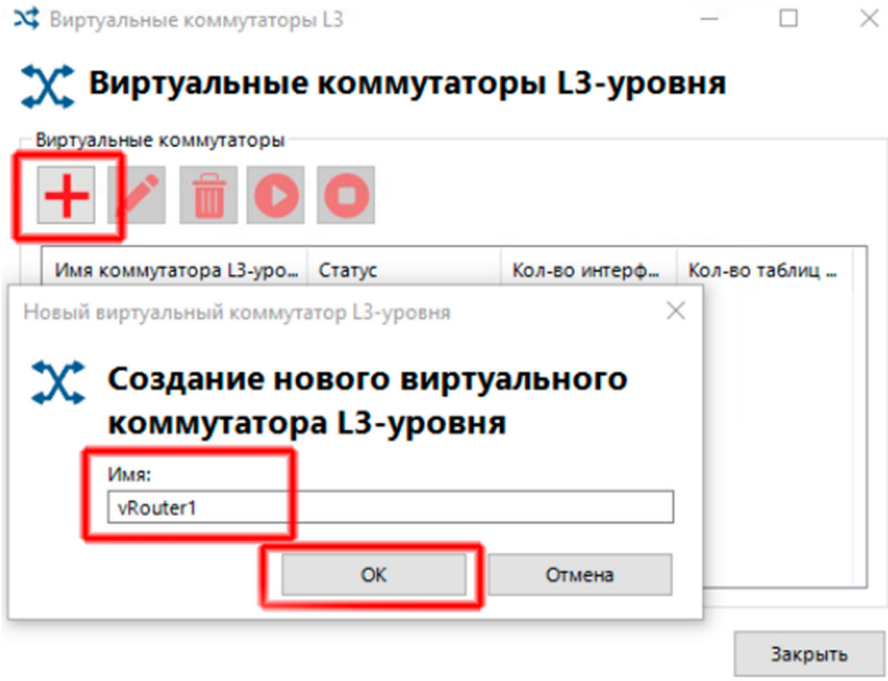
11. Создайте локальный мост от виртуального хаба «HubLocal» к сетевому интерфейсу «ens4»



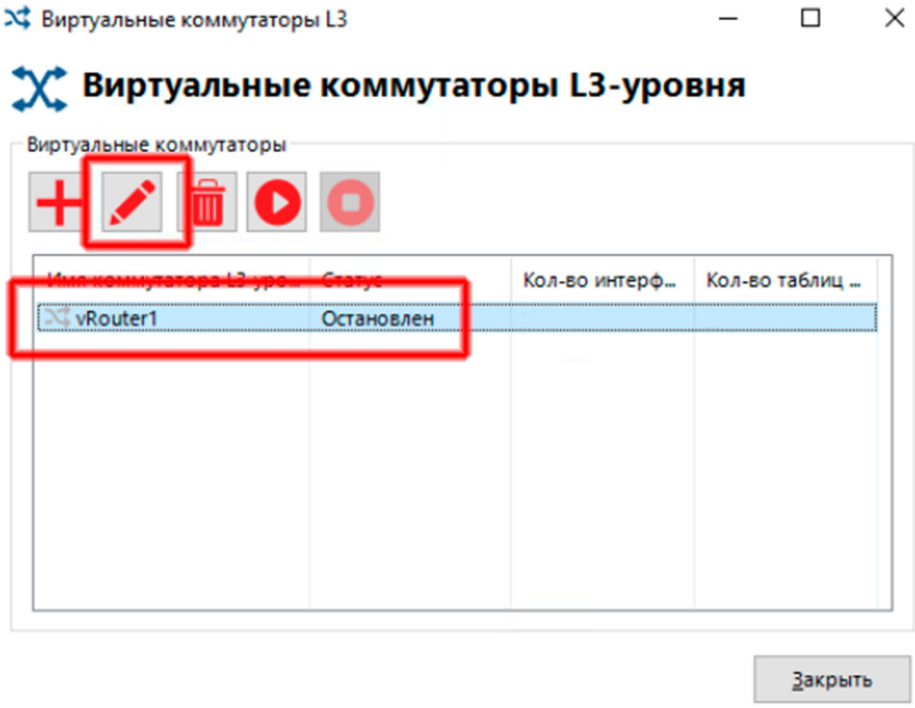
12. В настройках сервера зайдите в раздел «Коммутатор L3»



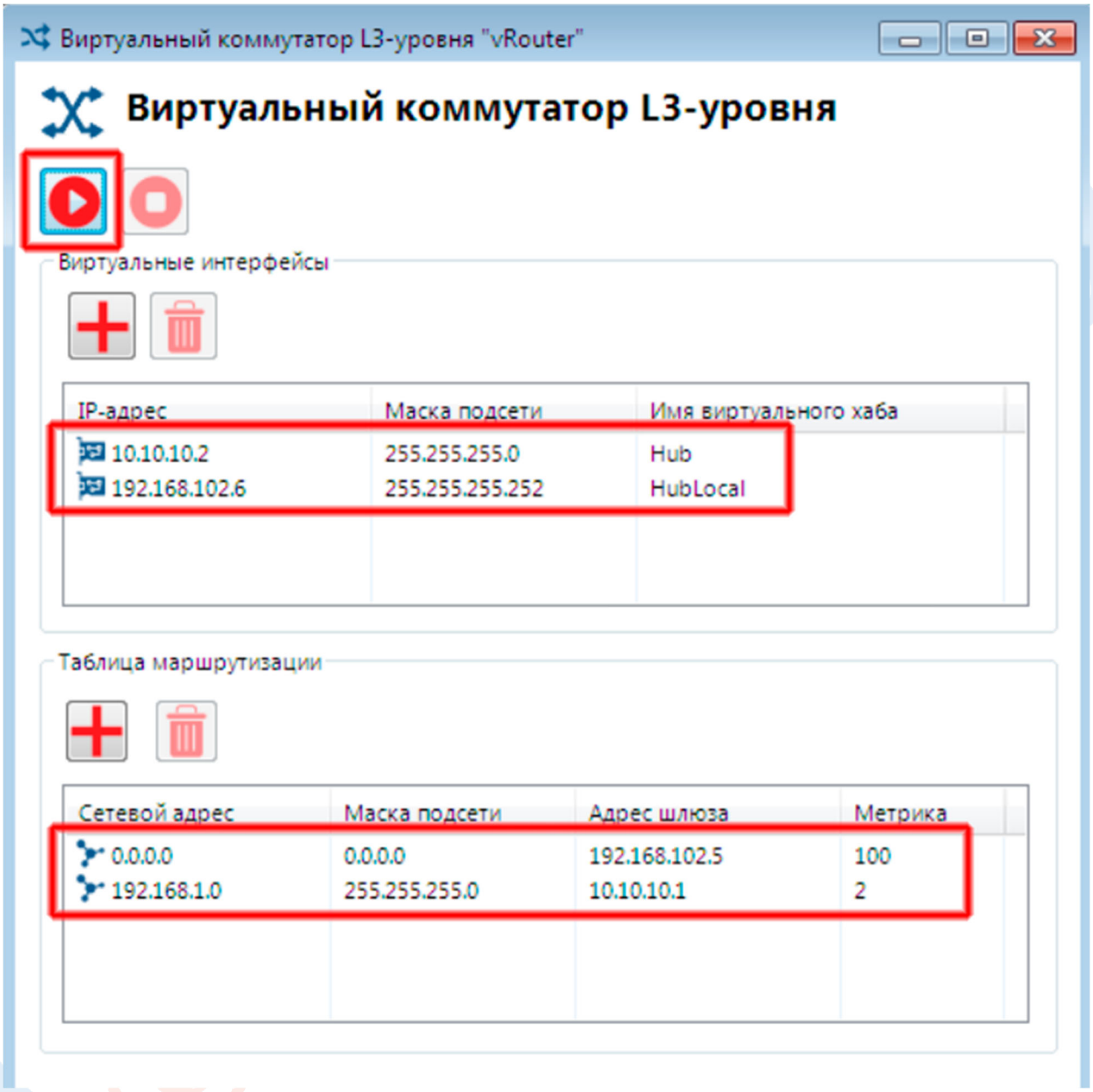
13. Нажмите «Добавить новый коммутатор», введите его имя и затем нажмите «ОК».



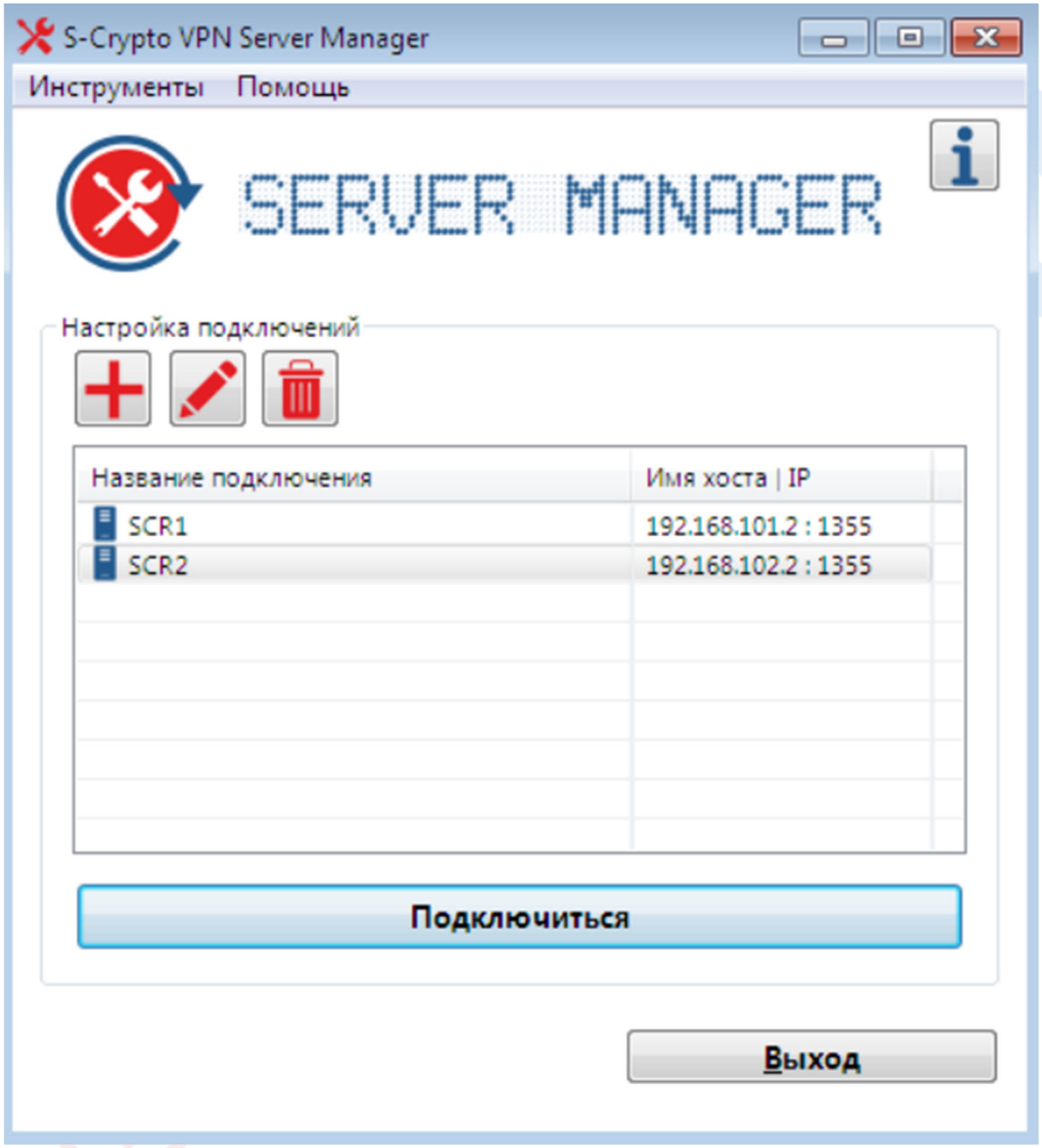
14. Зайдите в настройки созданного виртуального маршрутизатора



15. Настройте виртуальный маршрутизатор задав ip-адреса для каждого виртуального хаба, адрес шлюза по-умолчанию, маршрут к первой площадке. Затем включите виртуальный маршрутизатор нажатием кнопки «Активировать».

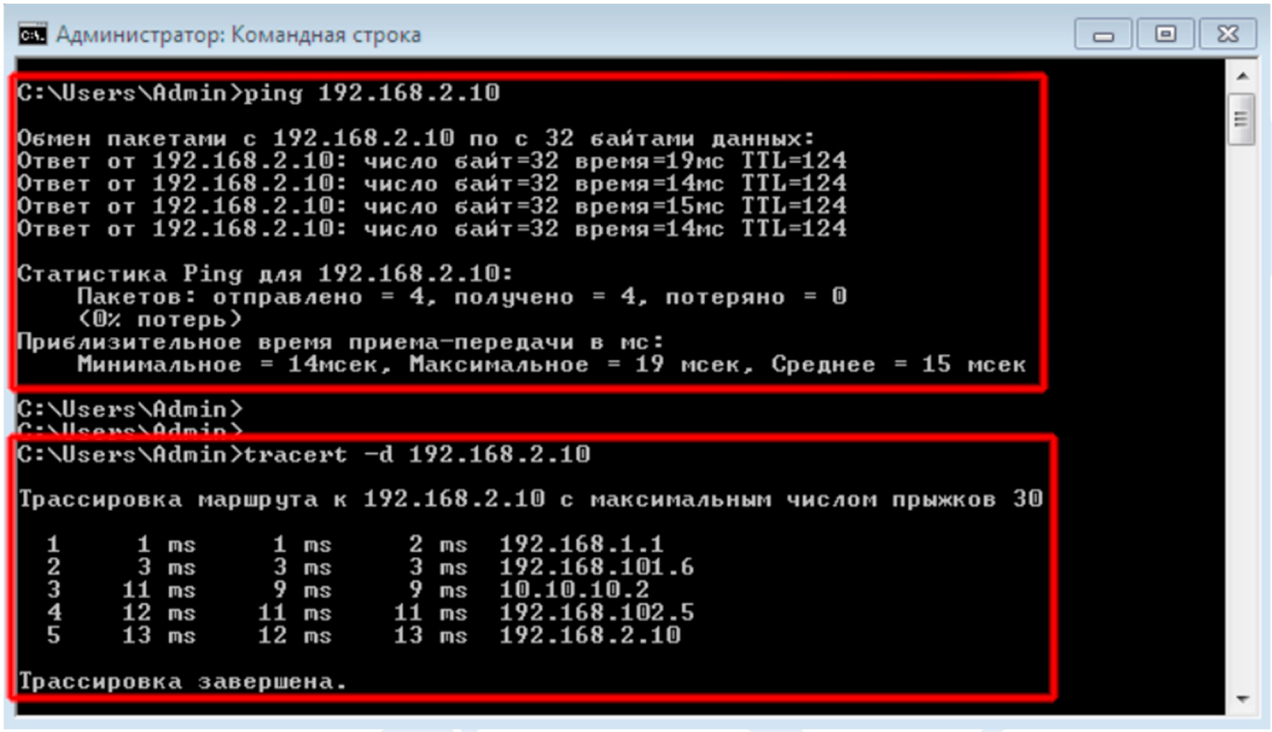


16. После установления защищенного соединения на устройстве администратора «Host1» можно создать новое подключение для удаленного администрирования устройства «SCR2» доступного через его интерфейс с ip-адресом 192.168.102.2



9. Проверка работоспособности стенда

1. Проверим доступность сетевых устройств второй площадки запустив с устройства «Host1» первой площадки команду «ping» на адрес устройства «Host2», а также командой «tracert» убедимся, что устройство доступно через защищенное соединение.



2. Проверим доступность сетевых устройств первой площадки запустив с устройства «Host2» второй площадки команду «ping» на адрес устройства «Host1», а также командой «tracert» убедимся, что устройство доступно через защищенное соединение.