

S-CRYPTO VPN 1.0

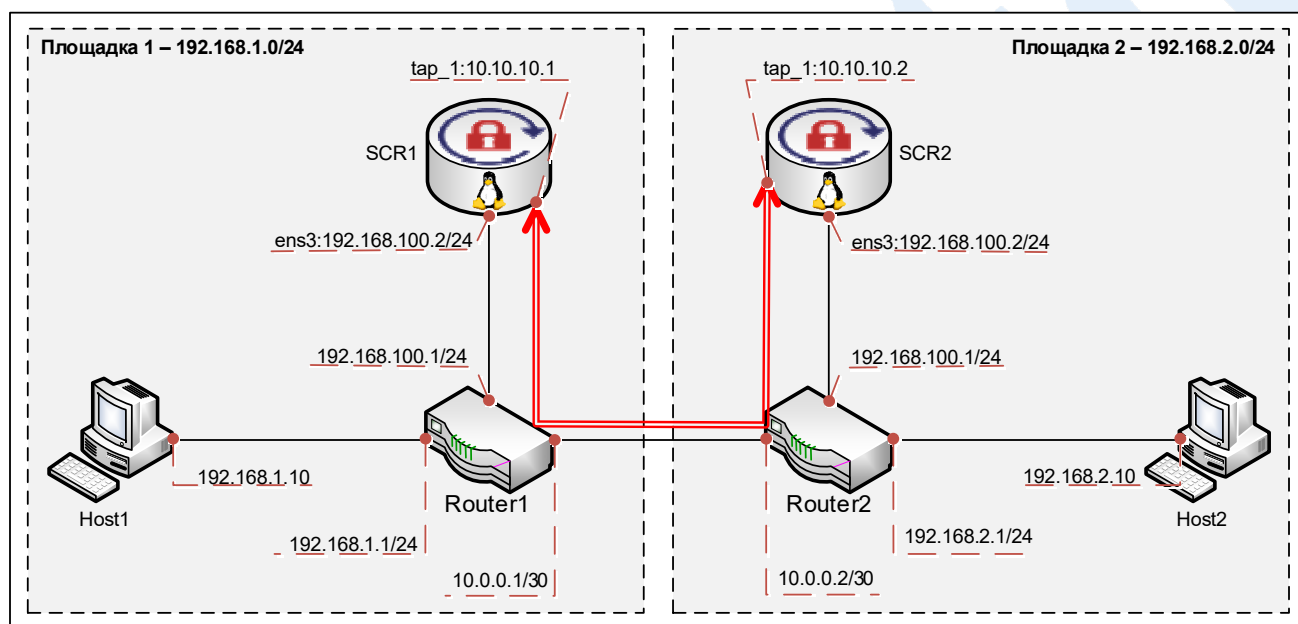
**Соединение между площадками (Site-to-Site).
Построение туннеля между двумя шлюзами
«S-Crypto VPN Server» на ОС Debian
подключенными методом Router-on-Stick
с маршрутизацией между защищаемыми
сегментами средствами операционной системы**

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»	3
7. Настройка шлюза безопасности «SCR1».....	4
8. Настройка шлюза безопасности «SCR2».....	8
9. Проверка работоспособности стенда.....	13

1. Описание стенда

Сценарий содержит пример настройки пары 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 операционной системы шлюзов безопасности «SCR1» и «SCR2».



2. Логика работы

В рамках сценария создание безопасного туннельного соединения будет производиться между виртуальными хабами, созданными на каждом из обоих шлюзов безопасности «SCR1» и «SCR2». Для осуществления маршрутизации средствами операционной системы от каждого виртуального хаба будет создан локальный мост к автоматически создаваемому в операционной системе виртуальному туннельному tap-интерфейсу. В приведенном сценарии шлюзы «SCR1» и «SCR2» подключены в центральные маршрутизаторы своих площадок через один интерфейс (методом on-Stick). Маршрутизаторы Router1 и Router2 направляют трафик, подлежащий шифрованию, на сетевой интерфейс шлюз безопасности своей площадки с помощью статического маршрута. Затем производится его шифрование и инкапсулированный трафик 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»

Устройство «Router1» – маршрутизатор, 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 ens3:192.168.100.2 шлюза безопасности «SCR1».

На сетевых интерфейсах устройства назначены статические ip-адреса в соответствии со схемой в разделе 1. Добавлены два статических маршрута: 192.168.2.0/24 via 192.168.100.2 и 10.10.10.0/24 via 192.168.100.2

6. Описание устройства «Router2»

Устройство «Router2» – маршрутизатор, обеспечивающий доступ устройств, находящихся в 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 192.168.100.2

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 в т.ч. tap-интерфейс, который будет создан позднее, а также сетевой маршрут ко второй площадке

Пример файла /etc/network/interfaces:

```
auto lo
iface lo inet loopback

allow-hotplug ens3
iface ens3 inet static
address 192.168.100.2
netmask 255.255.255.252
gateway 192.168.100.1

allow-hotplug tap_1
iface tap_1 inet static
address 10.10.10.1
netmask 255.255.255.0
post-up ip route add 192.168.2.0/24 via 10.10.10.2
pre-down ip route del 192.168.2.0/24 via 10.10.10.2
```

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». На виртуальном интерфейсе «tap_1» (будет создан позднее) назначен статический ip-адрес, на который поступает трафик из/в vpn-соединения для последующей маршрутизации в/из локальную сеть.

2. Разрешите пересылку пакетов между сетевыми интерфейсами. Для этого добавьте в файл /etc/sysctl.conf строку:

```
net.ipv4.ip_forward = 1
```

и примените изменения командой:

```
sudo sysctl -p
```

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

4. Дальнейшую настройку производите с устройства «Host1», предварительно настроив подключение программы «S-Crypto VPN Server Manager» к VPN-серверу «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/>.

5. С устройства «Host1» с помощью программы «S-Crypto VPN Server Manager» подключитесь к серверу «SCR1» по адресу 192.168.100.2 и создайте, если ещё не создан, виртуальный хаб «Hub» для терминирования входящих подключений

The screenshot shows the 'Новый виртуальный хаб' (New virtual hub) configuration window. It is divided into several sections:

- Виртуальный хаб (Virtual Hub):** Includes a field for 'Имя хаба:' (Hub name) with the value 'Hub' and a note '(только латинские буквы, цифры, спецсимволы)'. Below it is the 'Статус хаба:' (Hub status) section with radio buttons for 'Подключен' (Selected) and 'Отключен'.
- Администрирование (Administration):** Includes fields for 'Пароль администратора хаба:' and 'Подтвердите пароль:', both masked with dots. A note below the second field states '(мин. 6 символов, одна цифра и латинская буква)'. There is also a key icon.
- Классификация (Classification):** A note states 'В настоящее время сервер и виртуальный хаб работают в автономном(некластерном) режиме.' Below it are radio buttons for 'Статический хаб' and 'Динамический хаб'.
- Параметры хаба (Hub Parameters):** Includes a checkbox for 'Ограничить макс. количество сессий VPN' (Limit max. number of VPN sessions). Below it is a field for 'Макс. количество сессий:' (Max. number of sessions) with the value '0' and the unit 'сессий'. A note states 'Примечание: Без учета сессий созданных локальным мостом, виртуальным NAT или подключением к удаленной сети.' There is also a checkbox for 'Не отображать этот хаб анонимным пользователям'.

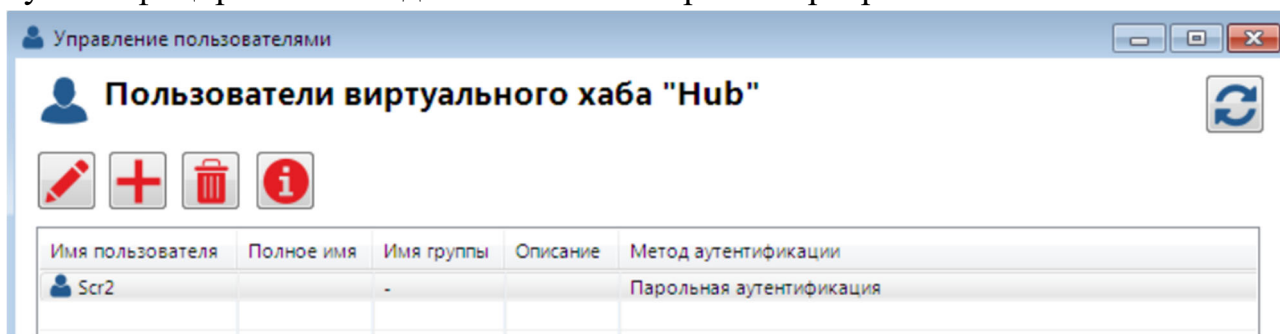
Buttons for 'ОК' and 'Отмена' are located at the bottom right.

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

The screenshot shows the 'Управление виртуальным хабом - 'Hub'' (Management of virtual hub - 'Hub') window. It features a large blue header with a gear icon and the title 'Виртуальный хаб 'Hub''.

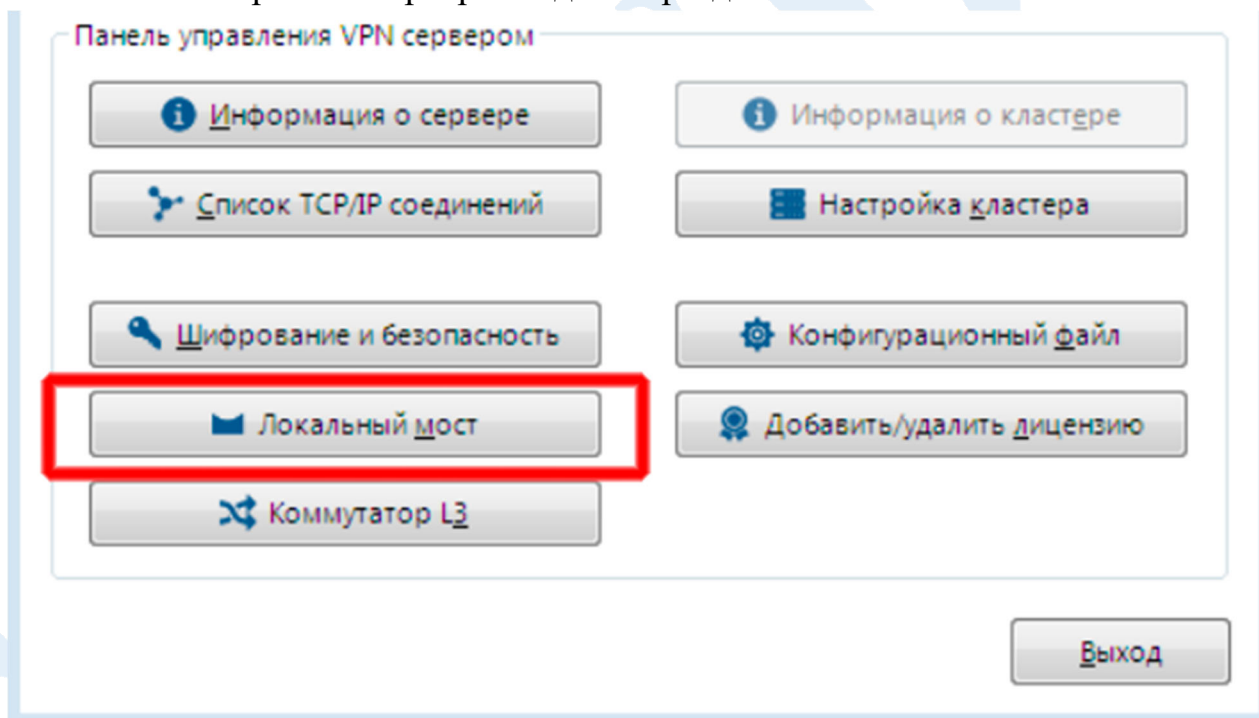
- Управление безопасностью (Security Management):** A red rectangle highlights the 'Пользователи' (Users) button. Other buttons in this section include 'Группы' (Groups) and 'Правила фильтрации пакетов' (Packet filtering rules).
- Информация о хаб (Hub Information):** A section on the right with a table-like structure. The header is 'Параметр' (Parameter). The table contains two rows: 'Имя хаба' (Hub name) and 'Статус' (Status).

7. 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/>

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



9. Создайте локальный мост от виртуального хаба «Hub» к виртуальному интерфейсу «1». Обратите внимание, что название виртуального интерфейса должно совпадать с названием интерфейса, после знака подчеркивания, которое было указано в пункте 1 раздела 7 этого сценария

Настройка локального моста

Настройка локального моста

Созданные локальные мосты

Номер	Имя виртуального хаба	Имя сетевого адаптера и...	Статус	MultiQueue
1	Hub	1	Онлайн	Нет

Создание нового локального моста

Виртуальный хаб:
Hub

Тип моста:

Мост с физическим сетевым адаптером

Мост с новым TAP-устройством

Имя нового TAP-устройства:
1 (< 11 символов)

Режим MultiQueue

Создать локальный мост

Примечание: Локальный мост устанавливает мостовое соединение L2-уровня между виртуальным хабом на этом VPN-сервере и физическим сетевым адаптером или виртуальным сетевым интерфейсом (TAP-устройством). Эта функция поддерживается только в Linux.

Настройка режима прозрачности для VLAN

Выйти

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 в т.ч. tap-интерфейс, который будет создан позднее, а также сетевой маршрут к первой площадке

Пример файла /etc/network/interfaces:

```
auto lo
iface lo inet loopback

allow-hotplug ens3
iface ens3 inet static
address 192.168.100.2
netmask 255.255.255.252
gateway 192.168.100.1

allow-hotplug tap_1
iface tap_1 inet static
address 10.10.10.2
netmask 255.255.255.0
post-up ip route add 192.168.1.0/24 via 10.10.10.1
pre-down ip route del 192.168.1.0/24 via 10.10.10.1
```

На интерфейсе «ens3» назначен статический ip-адрес, с которого иницируются подключения к шлюзу «SCR1». На виртуальном интерфейсе «tap_1» (будет создан позднее) назначен статический ip-адрес, на который поступает трафик из/в vpn-соединения для последующей маршрутизации в/из локальную сеть.

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

3. Первоначальную настройку производите с устройства «Host2», предварительно настроив подключение программы «S-Crypto VPN Server Manager» к VPN-серверу «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 192.168.100.2 и создайте, если ещё не создан, виртуальный хаб «Hub» от 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

Параметры VPN-подключения to SCR1

Настройка VPN-соединения

Название: to SCR1

Целевой VPN-сервер

Имя хоста | IP: 10.0.0.1

Номер TCP-порта: 1355 Отключить NAT-T

Имя виртуального хаба: Hub

Предварительно распределенный ключ (при наличии):

Прокси

Тип прокси:

Нет

HTTP

SOCKS4

SOCKS5

Настройка прокси

Импорт настроек прокси из IE

Настройка политики безопасности

Определение политики безопасности

Политика безопасности

Дополнительные параметры

Настройка дополнительных параметров...

Проверка сертификата целевого сервера

Всегда проверять сертификат VPN-сервера

Управление сертификатами откр. ключей

Указать сертификат сервера

Показать сертификат сервера

Аутентификация пользователя

Тип аутентификации: Парольная аутентификация

Имя пользователя: Scr2

Пароль:

Настройка переключения

Автоматическое переключение

Число попыток подключений: раз

Без ограничения

Интервал между попытками: 10 секунд

OK Отмена

8. После нажатия кнопки «ОК» активируйте созданное подключение

Соединения с удаленными сетями хаба Hub

Соединения с удаленными сетями

+

✎

🗑

🔌

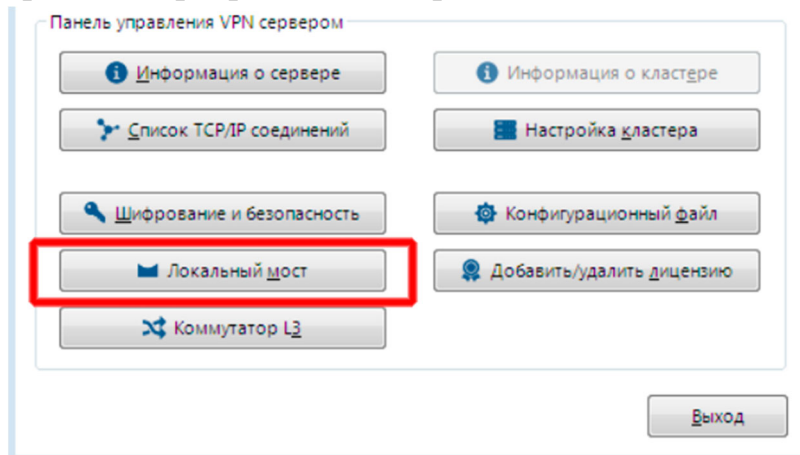
🚫

ℹ

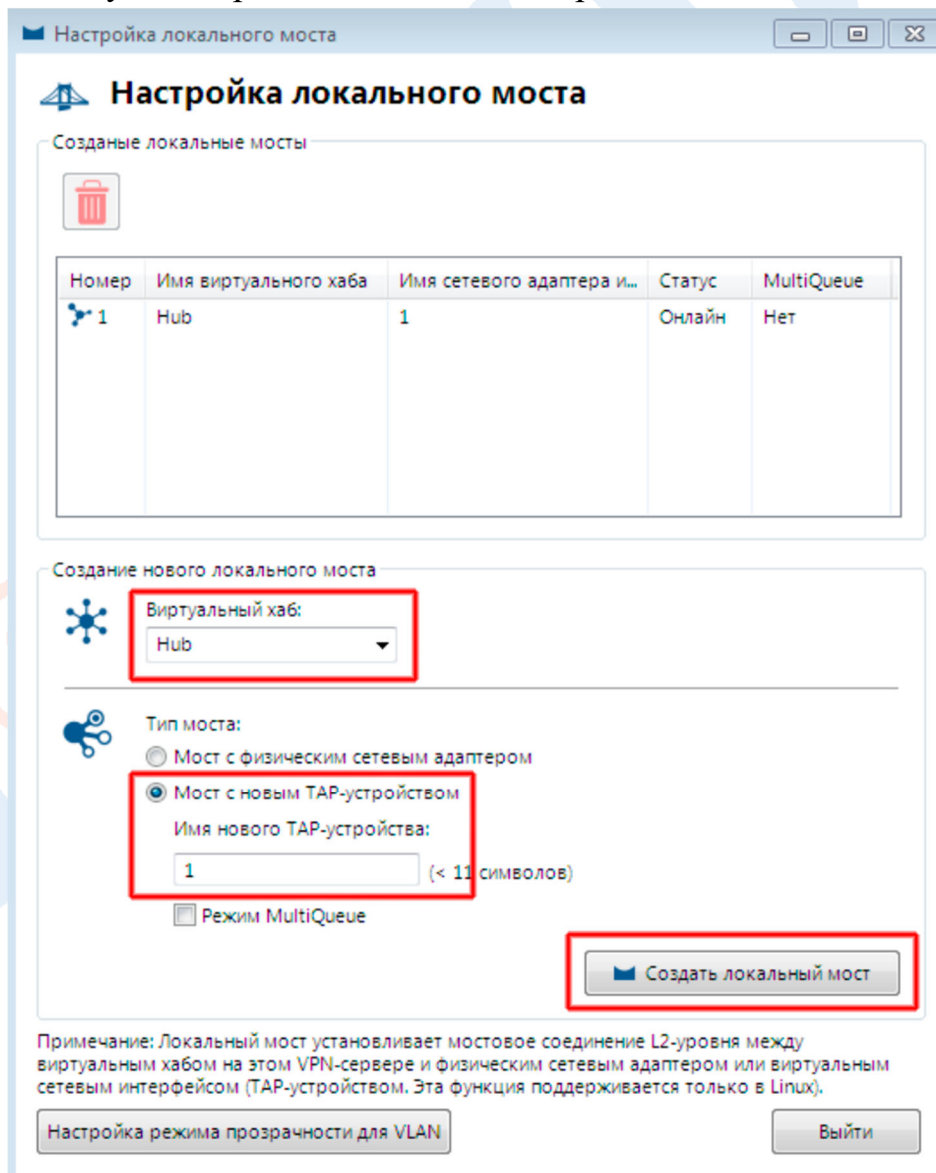
🗨

Название	Статус	Подключен с	Целевой VPN-сервер
to SCR1	Онлайн (соединен)	2024.08.30(Пт) 15:03:50	10.0.0.1

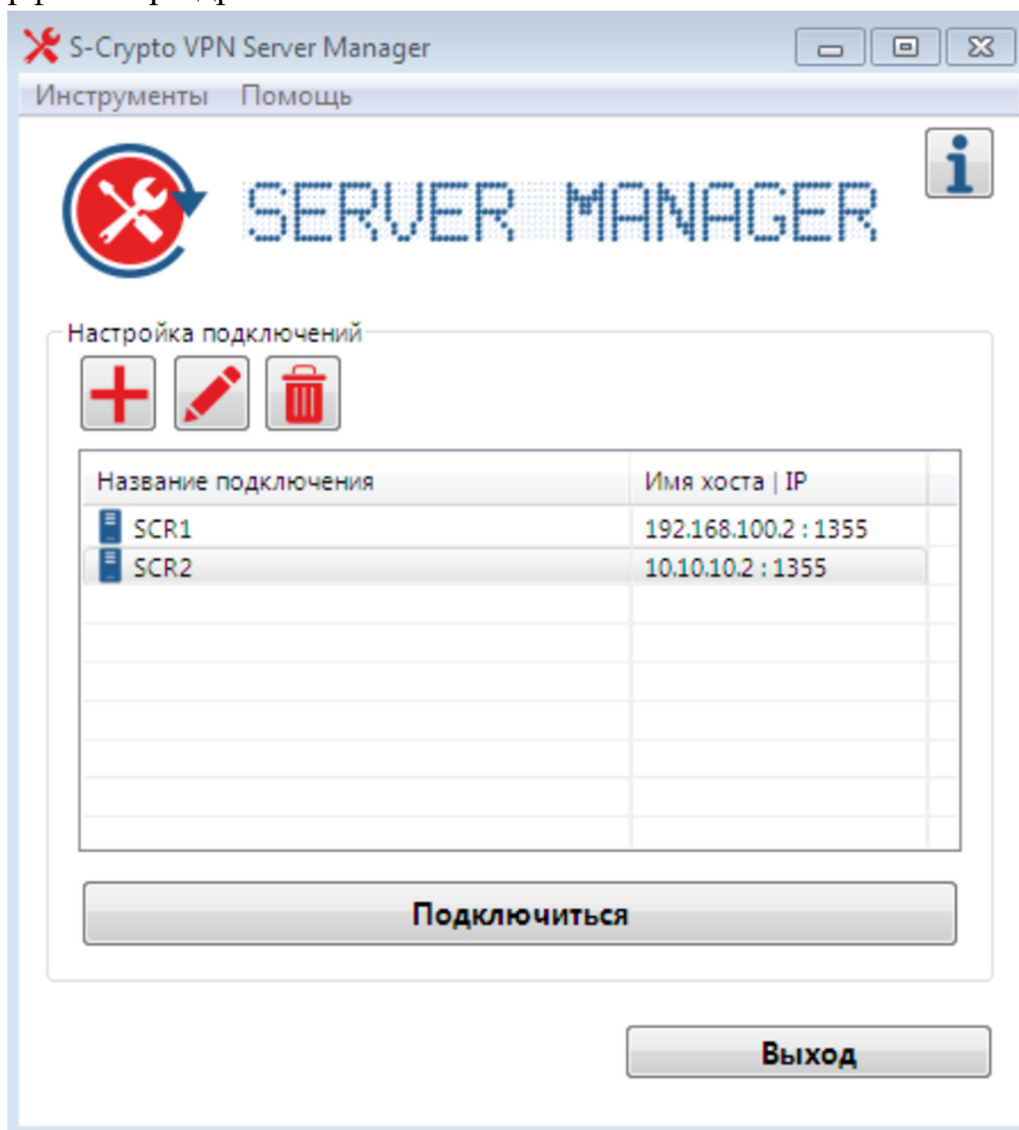
9. В настройках сервера зайдите в раздел «Локальный мост»



10. Создайте локальный мост от виртуального хаба «Hub» к виртуальному интерфейсу «1». Обратите внимание, что название виртуального интерфейса должно совпадать с названием интерфейса, после знака подчеркивания, которое было указано в пункте 1 раздела 8 этого сценария

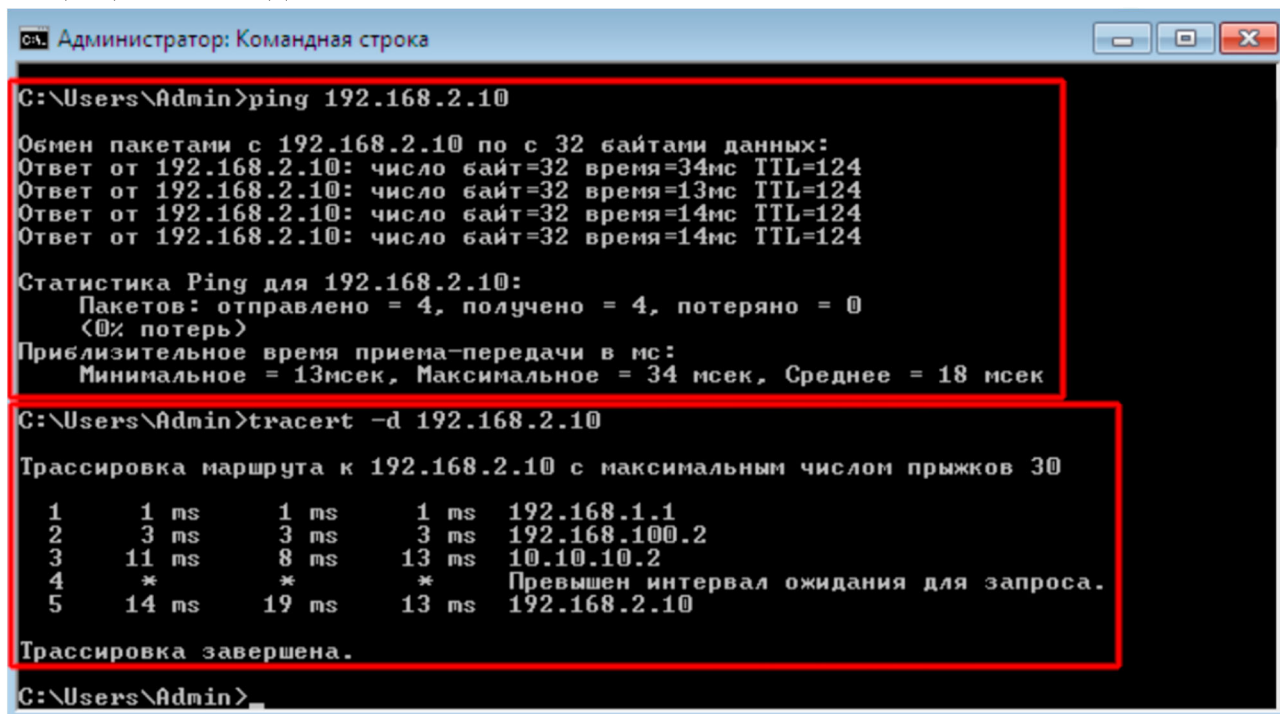


11. После установления защищенного соединения на устройстве администратора «Host1» можно создать новое подключение для удаленного администрирования устройства «SCR2» доступного через его виртуальный tap-интерфейс с ip-адресом 10.10.10.2



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.



```
Администратор: Командная строка
C:\Users\Admin>ping 192.168.2.10

Обмен пакетами с 192.168.2.10 по с 32 байтами данных:
Ответ от 192.168.2.10: число байт=32 время=34мс TTL=124
Ответ от 192.168.2.10: число байт=32 время=13мс TTL=124
Ответ от 192.168.2.10: число байт=32 время=14мс TTL=124
Ответ от 192.168.2.10: число байт=32 время=14мс TTL=124

Статистика Ping для 192.168.2.10:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (<0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 13мсек, Максимальное = 34 мсек, Среднее = 18 мсек

C:\Users\Admin>tracert -d 192.168.2.10

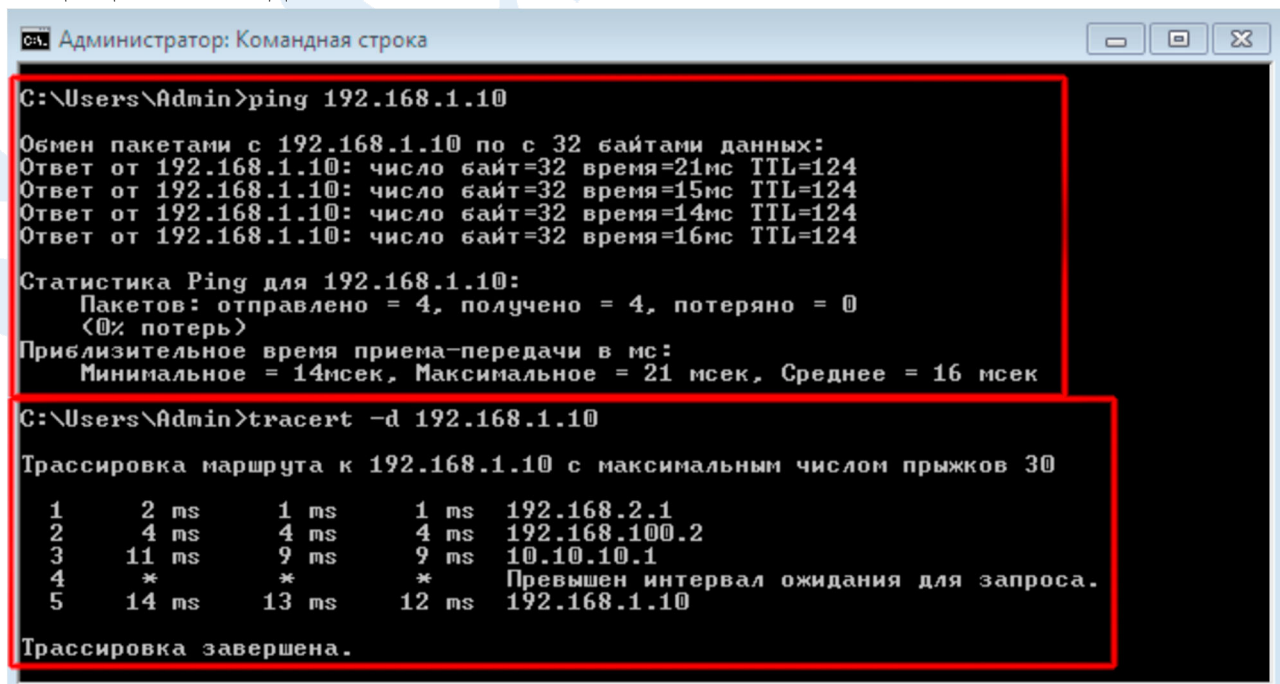
Трассировка маршрута к 192.168.2.10 с максимальным числом прыжков 30

 1      1 ms      1 ms      1 ms     192.168.1.1
 2      3 ms      3 ms      3 ms     192.168.100.2
 3     11 ms      8 ms     13 ms     10.10.10.2
 4      *         *         *         Превышен интервал ожидания для запроса.
 5     14 ms     19 ms     13 ms     192.168.2.10

Трассировка завершена.

C:\Users\Admin>
```

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.



```
Администратор: Командная строка
C:\Users\Admin>ping 192.168.1.10

Обмен пакетами с 192.168.1.10 по с 32 байтами данных:
Ответ от 192.168.1.10: число байт=32 время=21мс TTL=124
Ответ от 192.168.1.10: число байт=32 время=15мс TTL=124
Ответ от 192.168.1.10: число байт=32 время=14мс TTL=124
Ответ от 192.168.1.10: число байт=32 время=16мс TTL=124

Статистика Ping для 192.168.1.10:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (<0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 14мсек, Максимальное = 21 мсек, Среднее = 16 мсек

C:\Users\Admin>tracert -d 192.168.1.10

Трассировка маршрута к 192.168.1.10 с максимальным числом прыжков 30

 1       2 ms      1 ms      1 ms     192.168.2.1
 2       4 ms      4 ms      4 ms     192.168.100.2
 3      11 ms      9 ms      9 ms     10.10.10.1
 4      *         *         *         Превышен интервал ожидания для запроса.
 5      14 ms     13 ms     12 ms     192.168.1.10

Трассировка завершена.

C:\Users\Admin>
```