

S-CRYPTO VPN 1.0

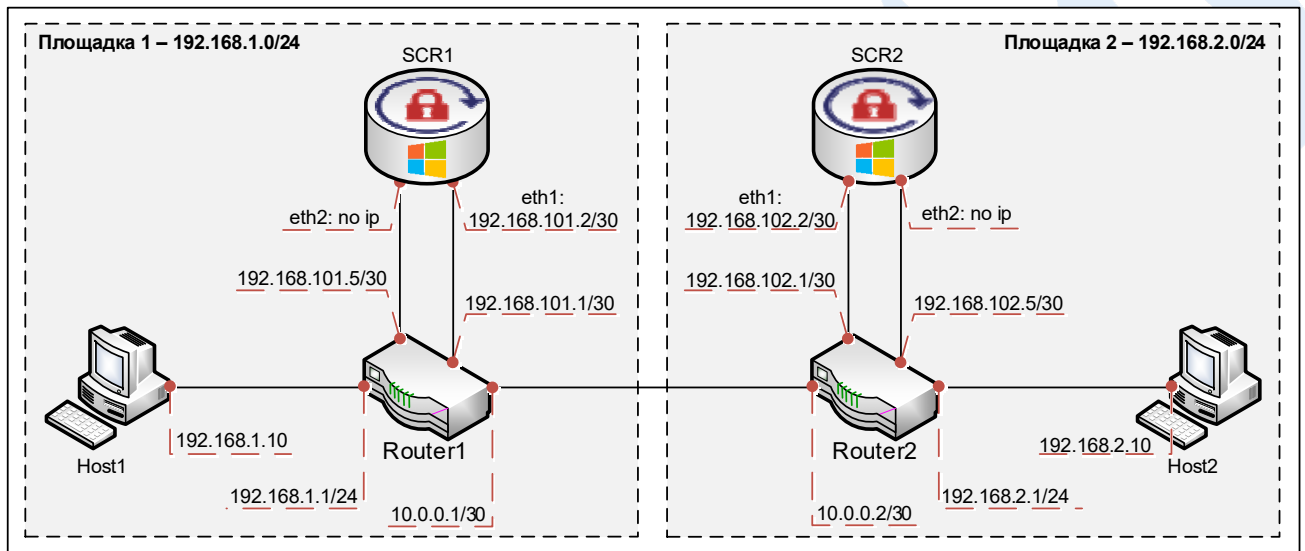
**Соединение между площадками (Site-to-Site).
Построение туннеля между двумя шлюзами
«S-Crypto VPN Server» на ОС Windows
с маршрутизацией между защищаемыми
сегментами встроенным виртуальным
маршрутизатором**

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».....	11
9. Проверка работоспособности стенда.....	19

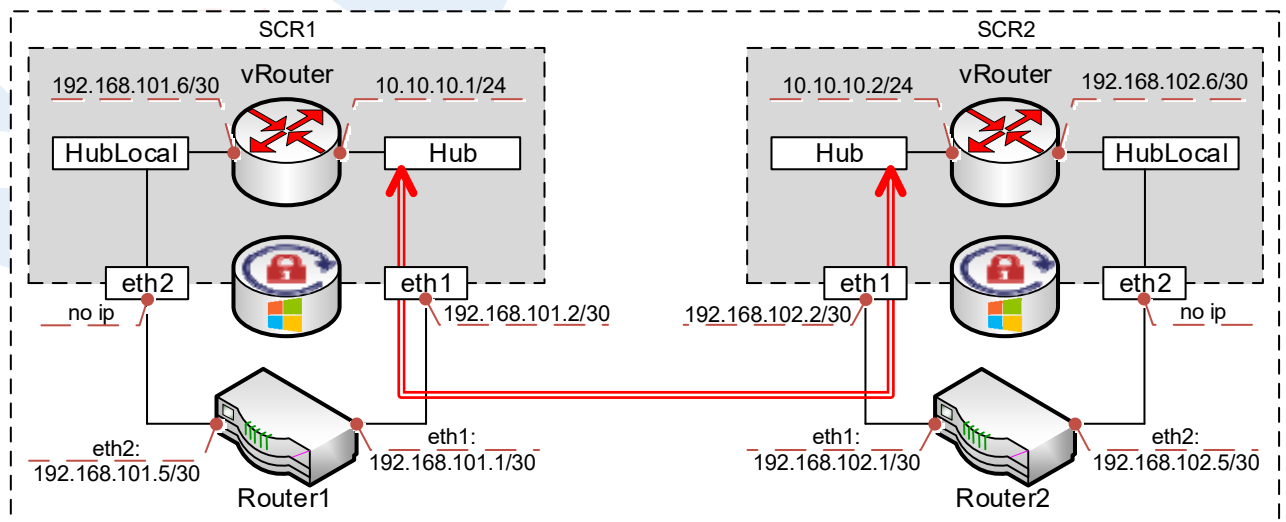
1. Описание стенда

Сценарий содержит пример настройки шлюзов безопасности «S-Crypto VPN Server», установленных на операционной системе Windows, 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 «eth2», шлюза безопасности своей площадки. Затем с помощью виртуального маршрутизатора трафик поступает на виртуальный хаб «Hub» и после шифрования инкапсулированный трафик через интерфейс «eth1» 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 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 eth1:192.168.101.2 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».

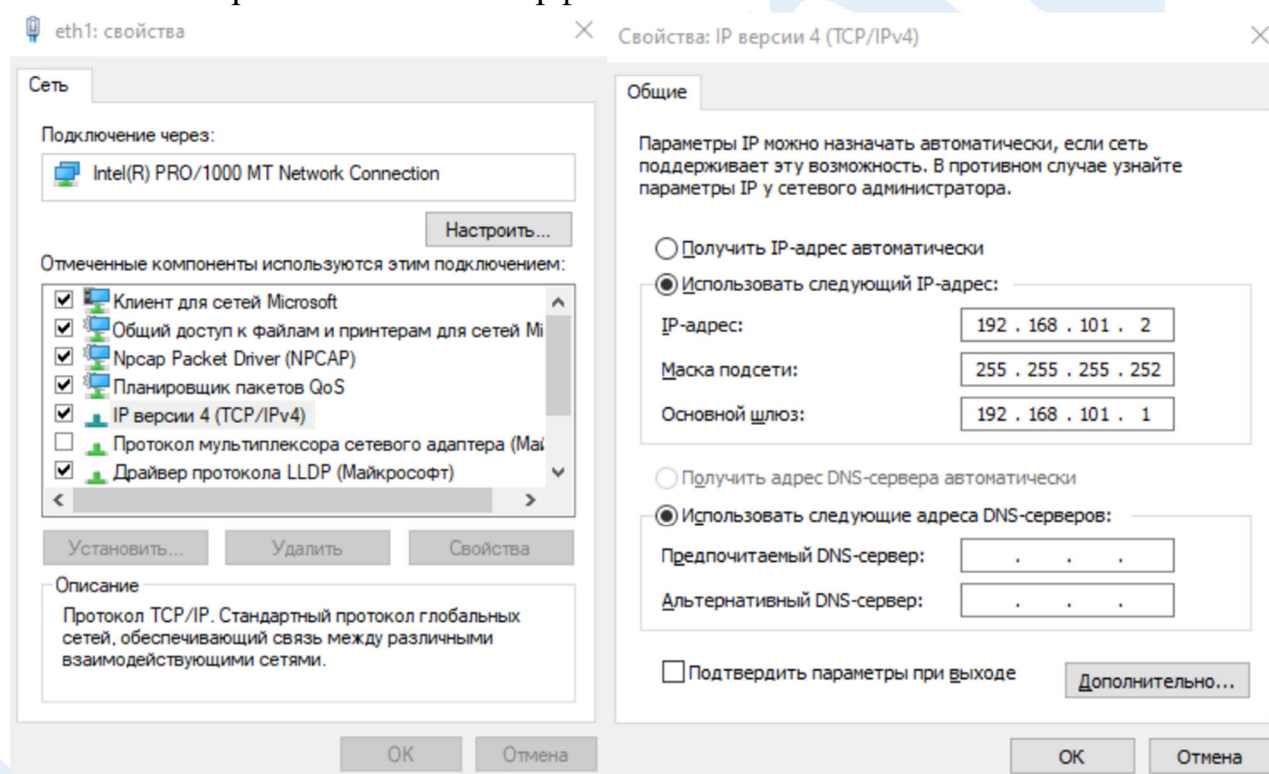
6. Описание устройства «Router2»

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

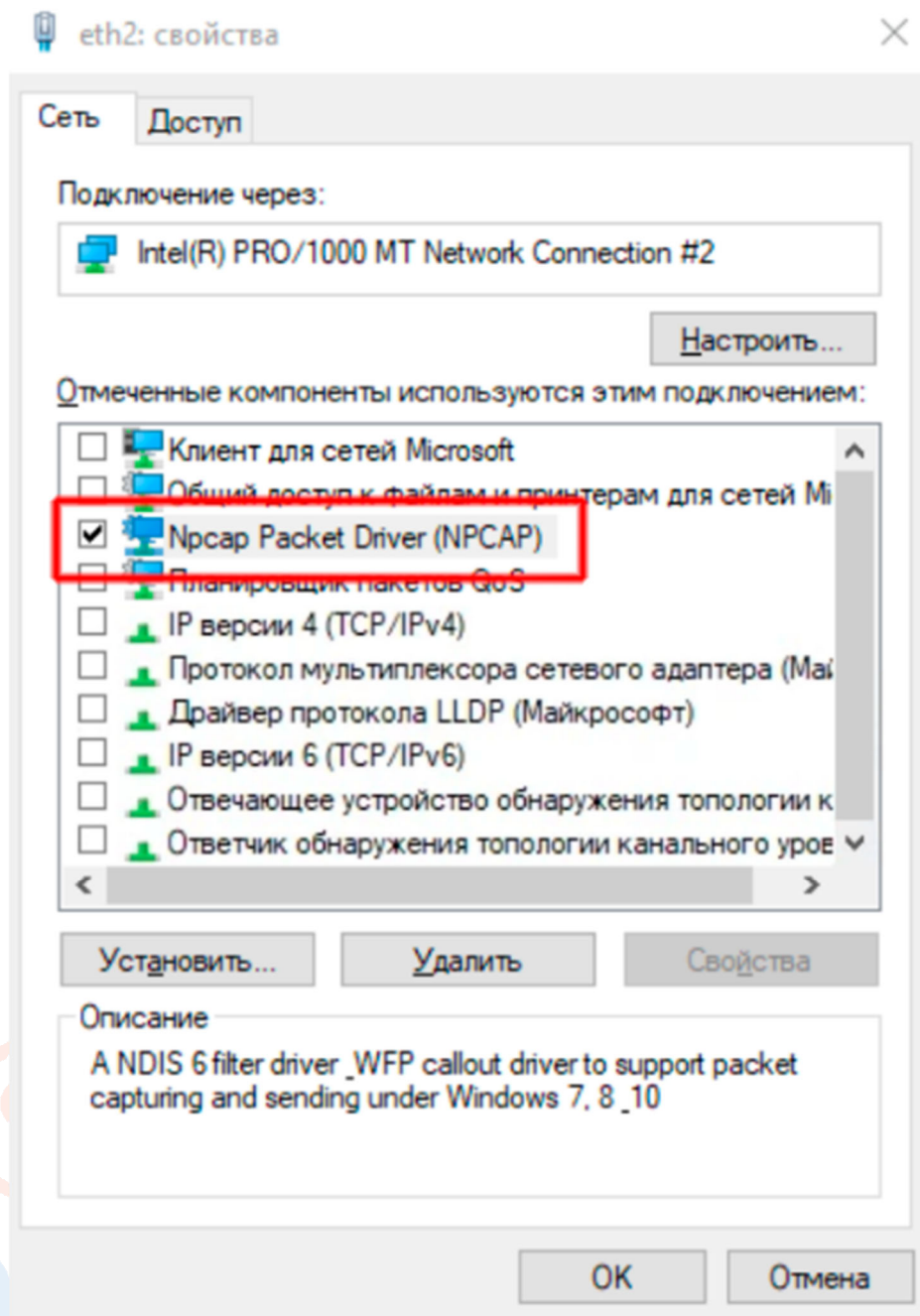
7. Настройка шлюза безопасности «SCR1»

Шлюз безопасности «SCR1» – устройство на базе операционной системы Windows 10 с установленными продуктами «S-Crypto VPN Server» и «S-Crypto VPN Server Manager».

1. Настройте сетевой интерфейс «eth1»



2. Настройте сетевой интерфейс «eth2». В связи с тем, что интерфейс используется в качестве «моста» в неразборчивом режиме, то для исключения проблем в маршрутизации трафика и повышения производительности отключите все неиспользуемые компоненты (по аналогии со скриншотом). Фильтр NPCAP будет установлен позднее и должен быть включен.



3. Установите программное обеспечение «S-Crypto VPN Server» и «S-Crypto VPN Server Manager» 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 помощью «S-Crypto VPN Server Manager» подключитесь к серверу и создайте виртуальный хаб «Hub» для терминирования входящих подключений

Новый виртуальный хаб

Виртуальный хаб

Имя хаба:
Hub
(только латинские буквы, цифры, спецсимволы)

Статус хаба:
 Подключен Отключен

Администрирование

Пароль администратора хаба:
.....

Подтвердите пароль:
.....
(мин. 6 символов, одна цифра и латинская буква)

Кластеризация

В настоящее время сервер и виртуальный хаб работают в автономном(некластерном) режиме.

Статический хаб Динамический хаб

Параметры хаба

Ограничить макс. количество сессий VPN

Макс. количество сессий:
..... сессий

Примечание: Без учета сессий созданных локальным мостом, виртуальным NAT или подключением к удаленной сети.

Не отображать этот хаб анонимным пользователям

OK Отмена

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

Управление виртуальным хабом - 'Hub'

Виртуальный хаб 'Hub'

Управление безопасностью

Пользователи

Группы

Правила фильтрации пакетов

Информация о хабе

Параметр

Имя хаба

Статус

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

Управление пользователями

Пользователи виртуального хаба "Hub"

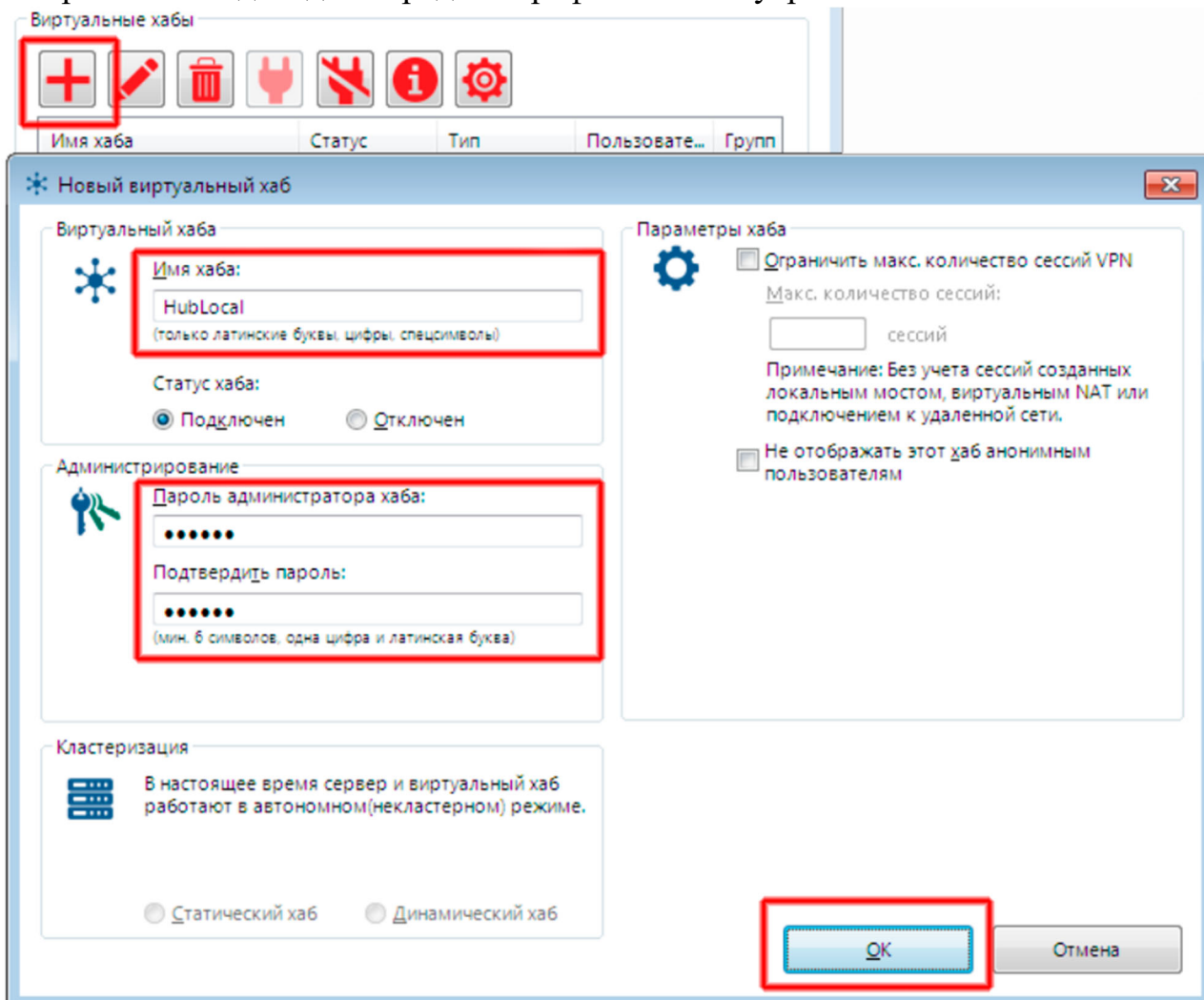
Имя пользователя Полное имя Имя группы Описание Метод аутентификации

Scr2		-		Парольная аутентификация
------	--	---	--	--------------------------

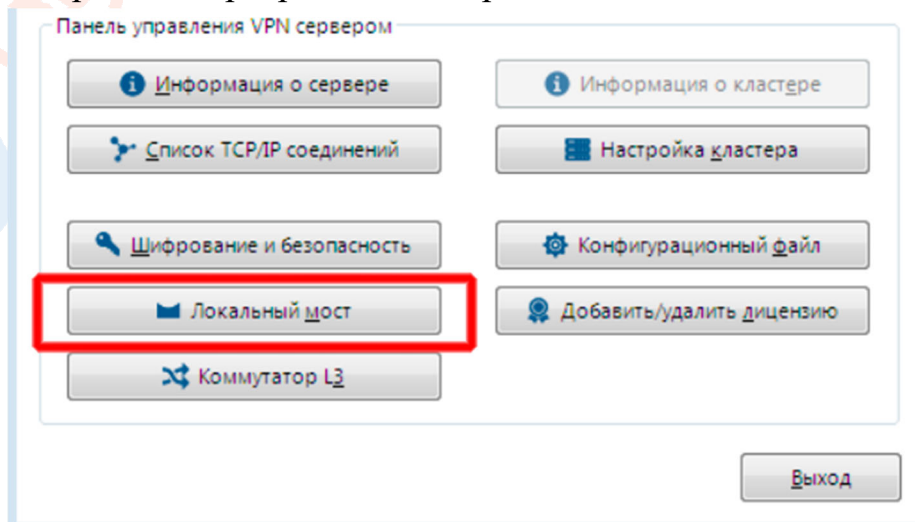
Информация о настройке различных способов аутентификации пользователей размещена в инструкции «Способы аутентификации» доступной на

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 «eth2»

Настройка локального моста

Настройка локального моста

Созданные локальные мосты

Номер	Имя виртуального хаба	Имя сетевого адаптера или TAP-устройства	Статус
1	HubLocal	Intel(R) PRO/1000 MT Network Connection #2 ...	Онлайн

Создание нового локального моста

Виртуальный хаб:
HubLocal

Тип моста:
 Мост с физическим сетевым адаптером

Сетевой адаптер:
eth2 [Intel(R) PRO/1000 MT Network Connection #2 (ID=3184092413)]

Примечание: Если недавно добавленный в систему сетевой адаптер не появляется в списке, перезагрузите компьютер и снова откройте этот экран.

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

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

Шифрование и безопасность

Конфигурационный файл

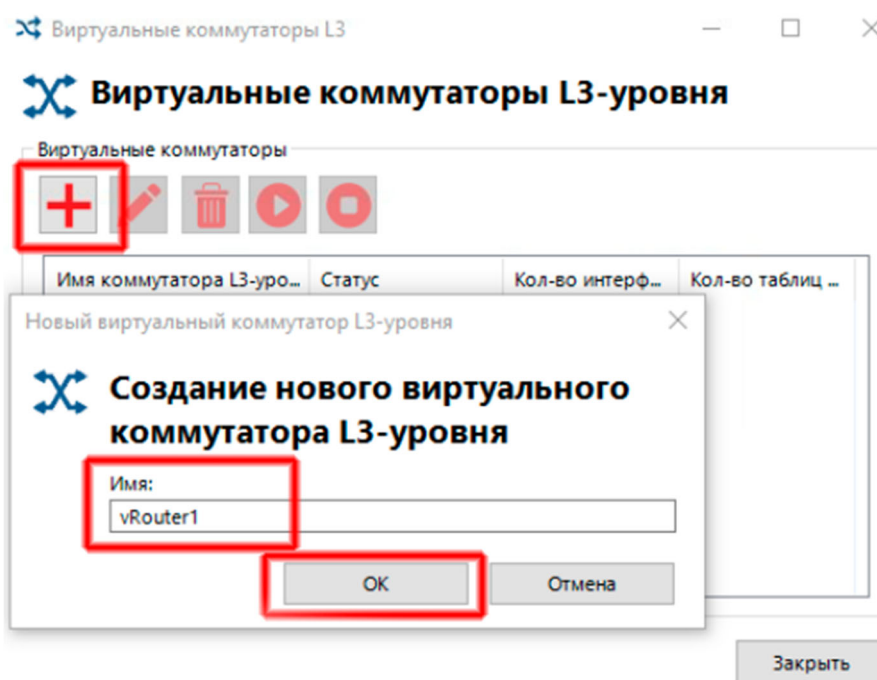
Локальный мост

Добавить/удалить лицензию

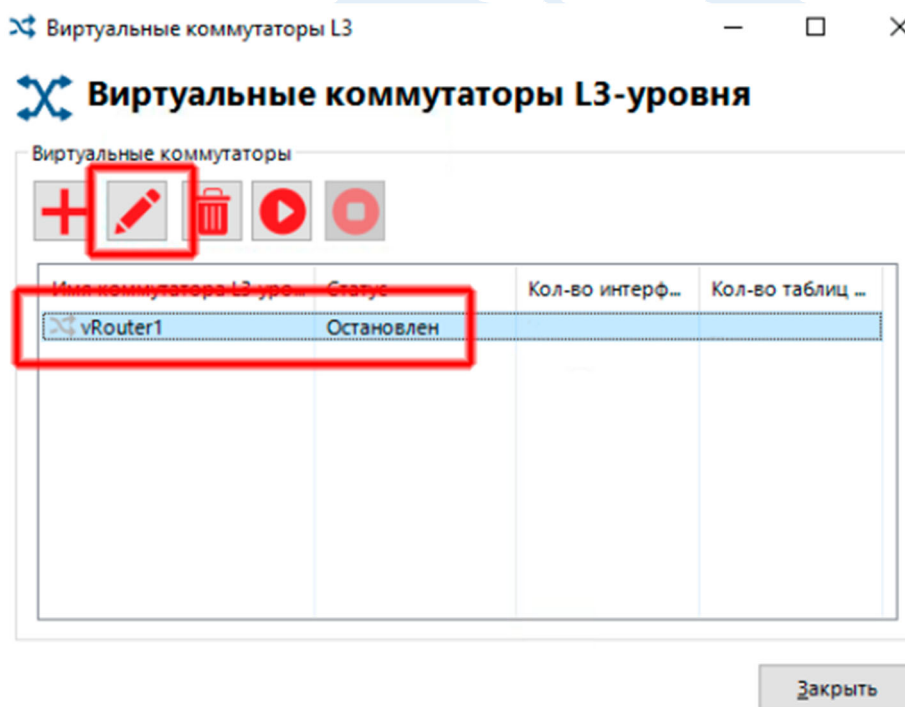
Коммутатор L3

Выход

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».

Виртуальный коммутатор L3-уровня

Виртуальные интерфейсы

IP-адрес	Маска подсети	Имя виртуального хаба
10.10.10.1	255.255.255.0	Hub
192.168.101.6	255.255.255.252	HubLocal

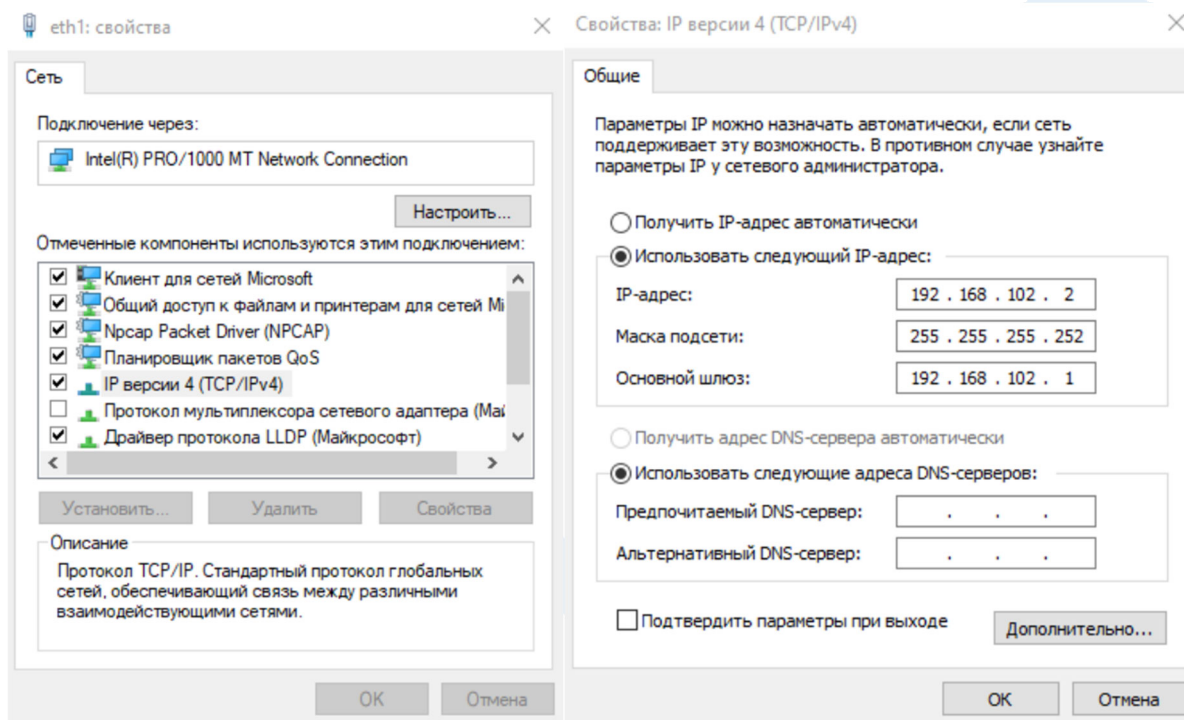
Таблица маршрутизации

Сетевой адрес	Маска подсети	Адрес шлюза	Метрика
0.0.0.0	0.0.0.0	192.168.101.5	100
192.168.2.0	255.255.255.0	10.10.10.2	2
192.168.102.2	255.255.255.255	10.10.10.2	2

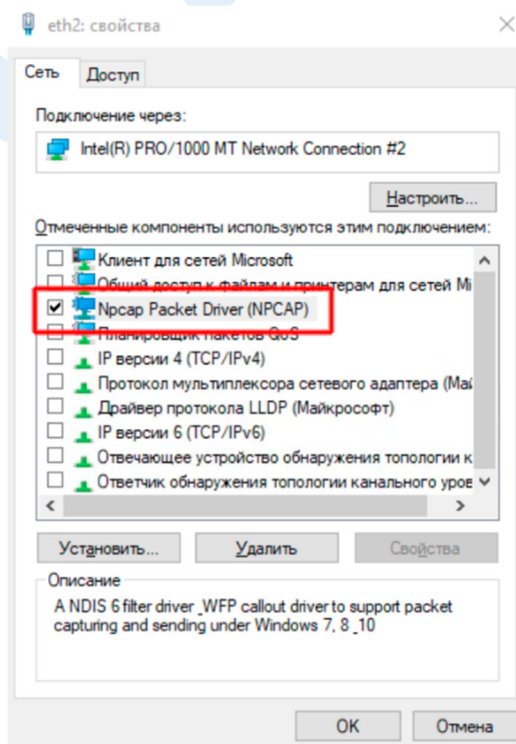
8. Настройка шлюза безопасности «SCR2»

Шлюз безопасности «SCR2» – устройство на базе операционной системы Windows 10 с установленными продуктами «S-Crypto VPN Server» и «S-Crypto VPN Server Manager».

1. Настройте сетевой интерфейс «eth1»

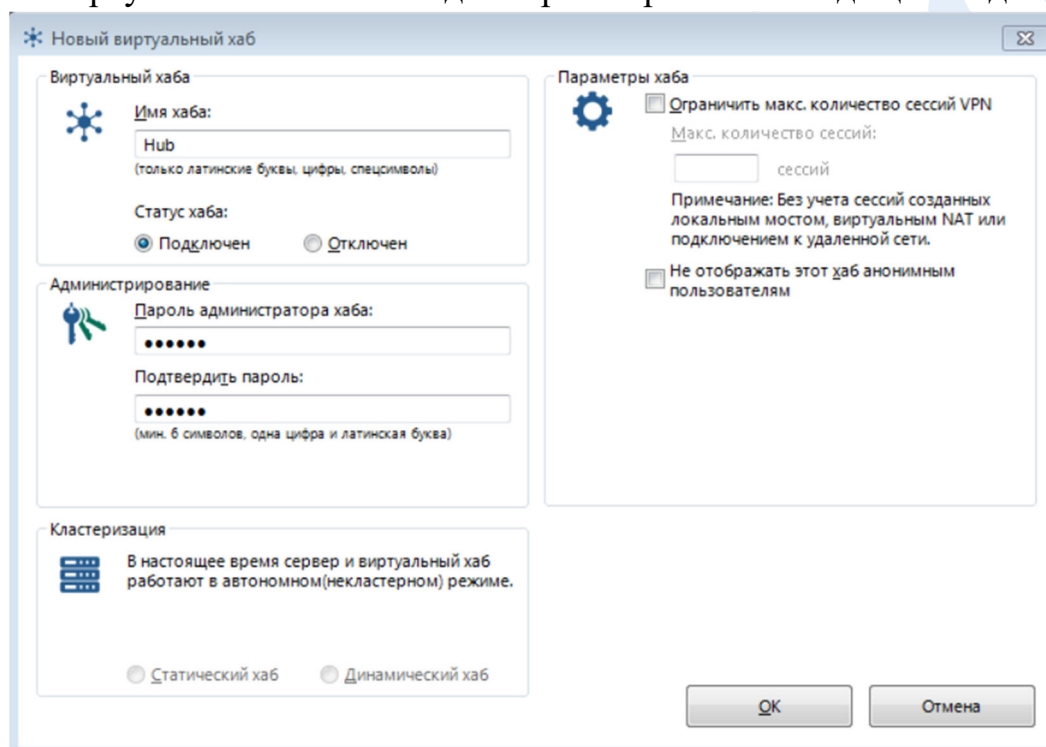


2. Настройте сетевой интерфейс «eth2». Отключите все неиспользуемые компоненты (по аналогии со скриншотом). Фильтр NPCAP будет установлен позднее и должен быть включен.

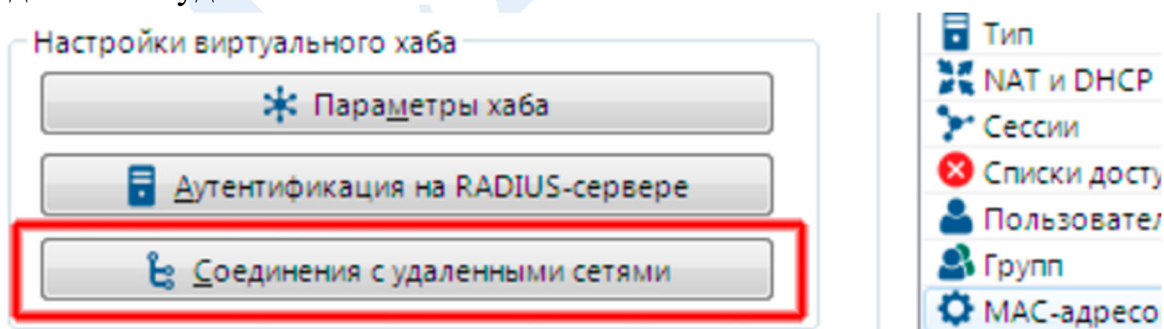


3. Установите программное обеспечение «S-Crypto VPN Server» и «S-Crypto VPN Server Manager» в соответствии с инструкцией «Руководство администратора», доступной в комплекте поставки, а также на официальном сайте компании в разделе «Техническая поддержка» - «Документация» <https://s-crypto.by/support-pages/documentation/>.

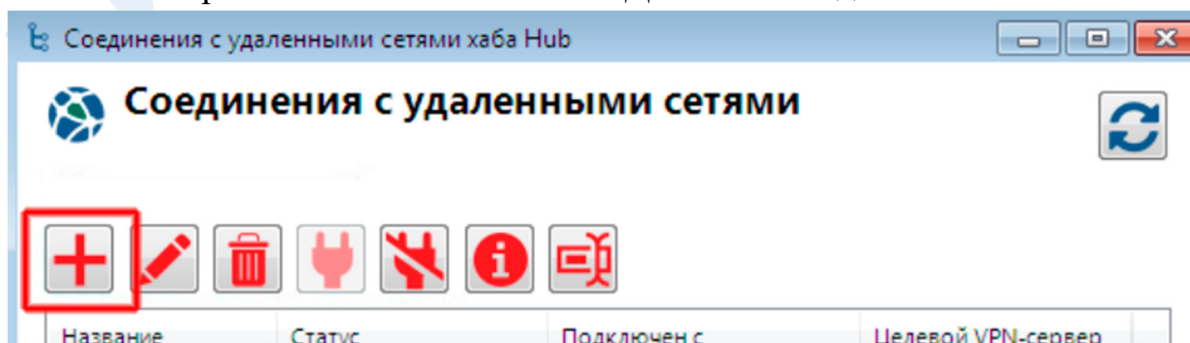
4. С помощью «S-Crypto VPN Server Manager» подключитесь к серверу и создайте виртуальный хаб «Hub» для терминиования входящих подключений



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 создайте новый виртуальный хаб «HubLocal», который необходим для передачи трафика в/из внутреннего сегмента

Виртуальные хабы

Имя хаба	Статус	Тип	Пользовате...	Групп
----------	--------	-----	---------------	-------

Новый виртуальный хаб

Виртуальный хаб

Имя хаба:
HubLocal
(только латинские буквы, цифры, спецсимволы)

Статус хаба:
 Подключен Отключен

Администрирование

Пароль администратора хаба:
.....

Подтвердите пароль:
.....
(мин. 6 символов, одна цифра и латинская буква)

Кластеризация

В настоящее время сервер и виртуальный хаб работают в автономном(некластерном) режиме.

Статический хаб Динамический хаб

Параметры хаба

Ограничить макс. количество сессий VPN

Макс. количество сессий:
..... сессий

Примечание: Без учета сессий созданных локальным мостом, виртуальным NAT или подключением к удаленной сети.

Не отображать этот хаб анонимным пользователям

OK Отмена

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

Панель управления VPN сервером

Информация о сервере

Информация о кластере

Список TCP/IP соединений

Настройка кластера

Шифрование и безопасность

Конфигурационный файл

Локальный мост

Добавить/удалить лицензию

Коммутатор L3

Выход

11. Создайте локальный мост от виртуального хаба «HubLocal» к сетевому интерфейсу «eth2»

Настройка локального моста

Настройка локального моста

Созданные локальные мосты

Номер	Имя виртуального хаба	Имя сетевого адаптера или TAP-устройства	Статус
1	HubLocal	Intel(R) PRO/1000 MT Network Connection #2 ...	Онлайн

Создание нового локального моста

Виртуальный хаб:
HubLocal

Тип моста:
 Мост с физическим сетевым адаптером

Сетевой адаптер:
eth2 [Intel(R) PRO/1000 MT Network Connection #2 (ID=3184092413)]

Примечание: Если недавно добавленный в систему сетевой адаптер не появляется в списке, перезагрузите компьютер и снова откройте этот экран.

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

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

Шифрование и безопасность

Конфигурационный файл

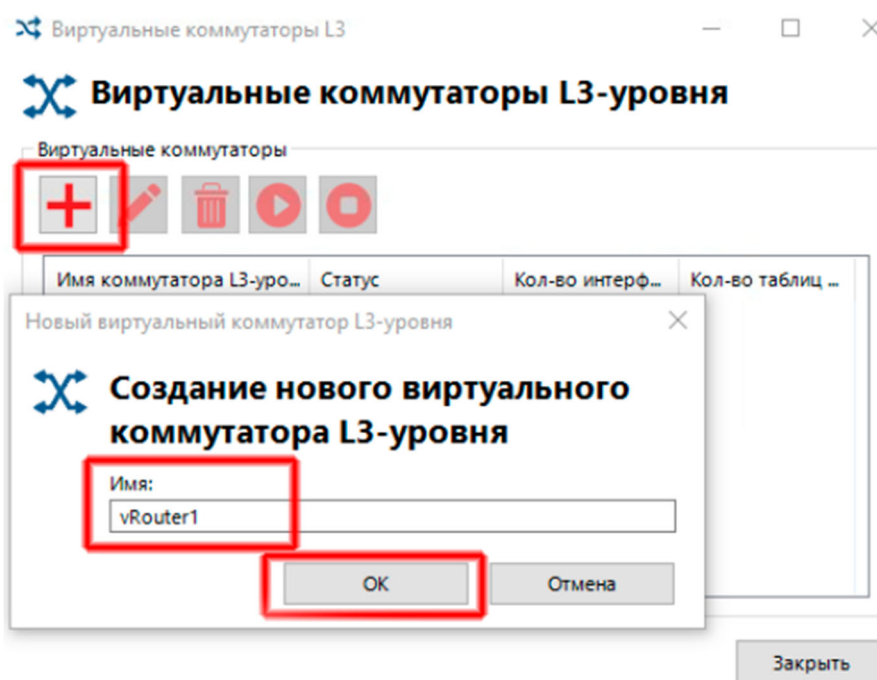
Локальный мост

Добавить/удалить лицензию

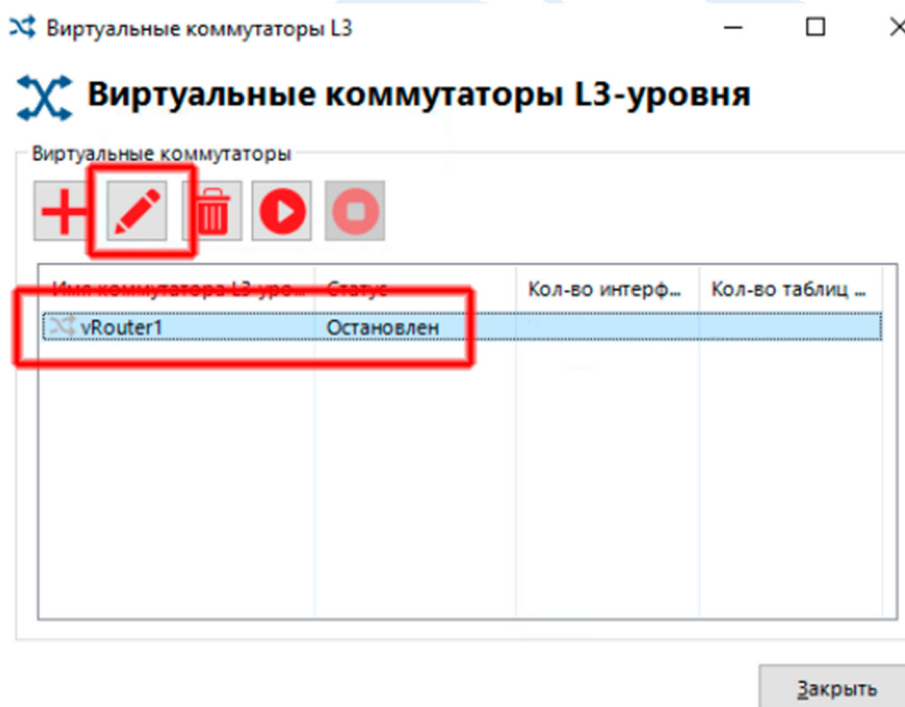
Коммутатор L3

Выход

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».

Виртуальный коммутатор L3-уровня "vRouter"

Виртуальный коммутатор L3-уровня

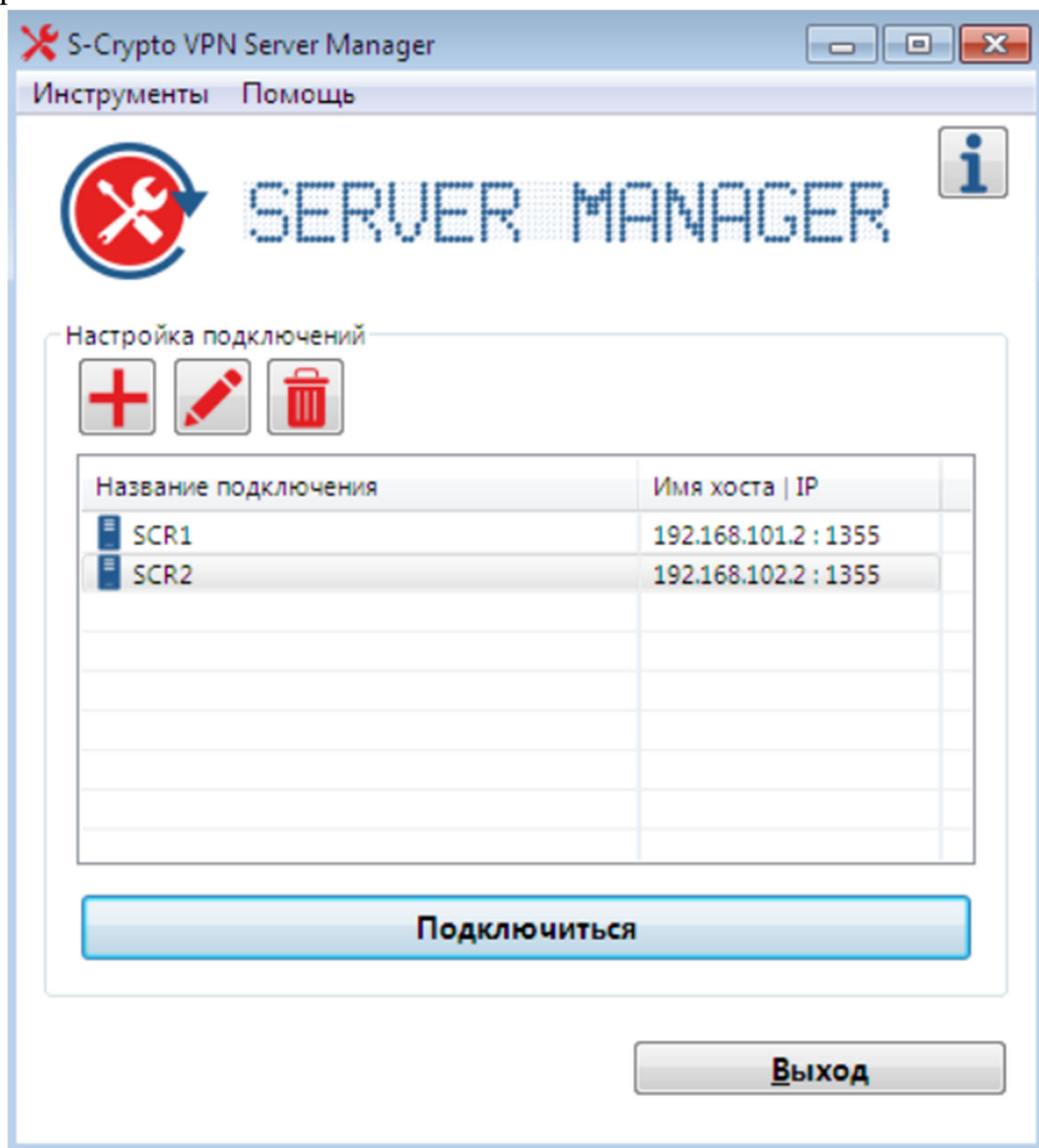
Виртуальные интерфейсы

IP-адрес	Маска подсети	Имя виртуального хаба
10.10.10.2	255.255.255.0	Hub
192.168.102.6	255.255.255.252	HubLocal

Таблица маршрутизации

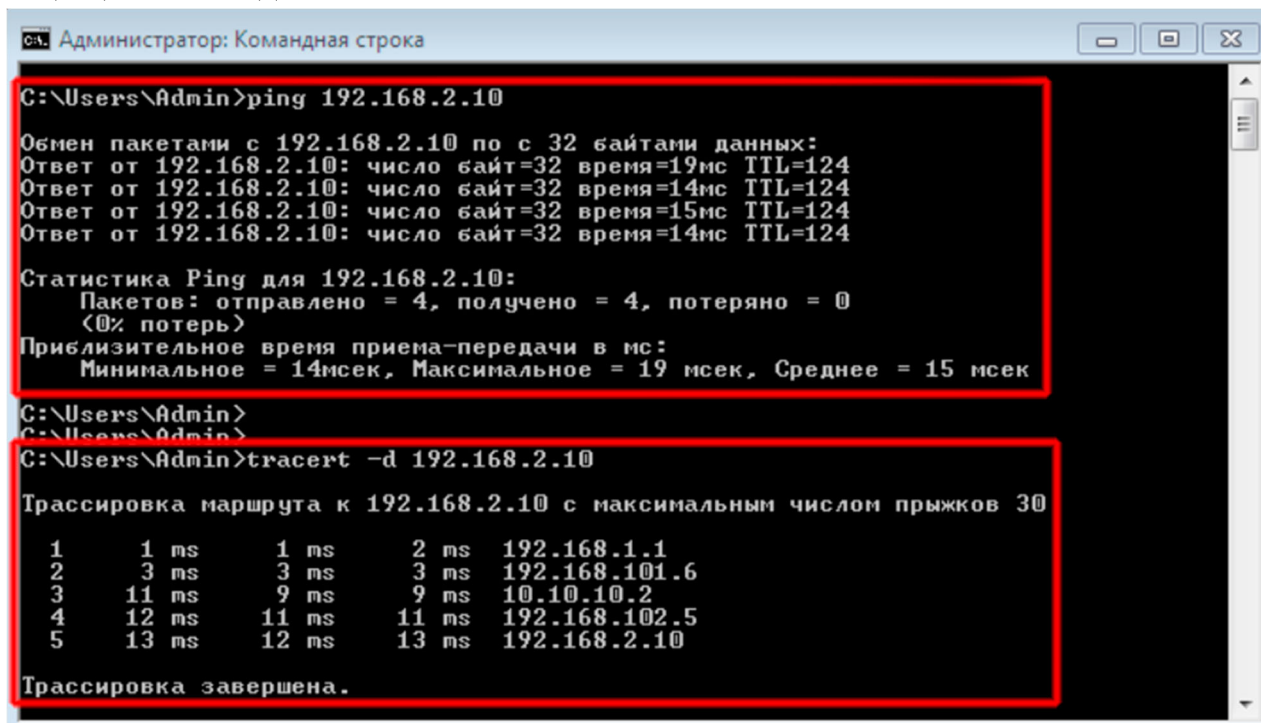
Сетевой адрес	Маска подсети	Адрес шлюза	Метрика
0.0.0.0	0.0.0.0	192.168.102.5	100
192.168.1.0	255.255.255.0	10.10.10.1	2

16. После установки 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.



```
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=19мс 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=15мс 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 = 14мсек, Максимальное = 19 мсек, Среднее = 15 мсек

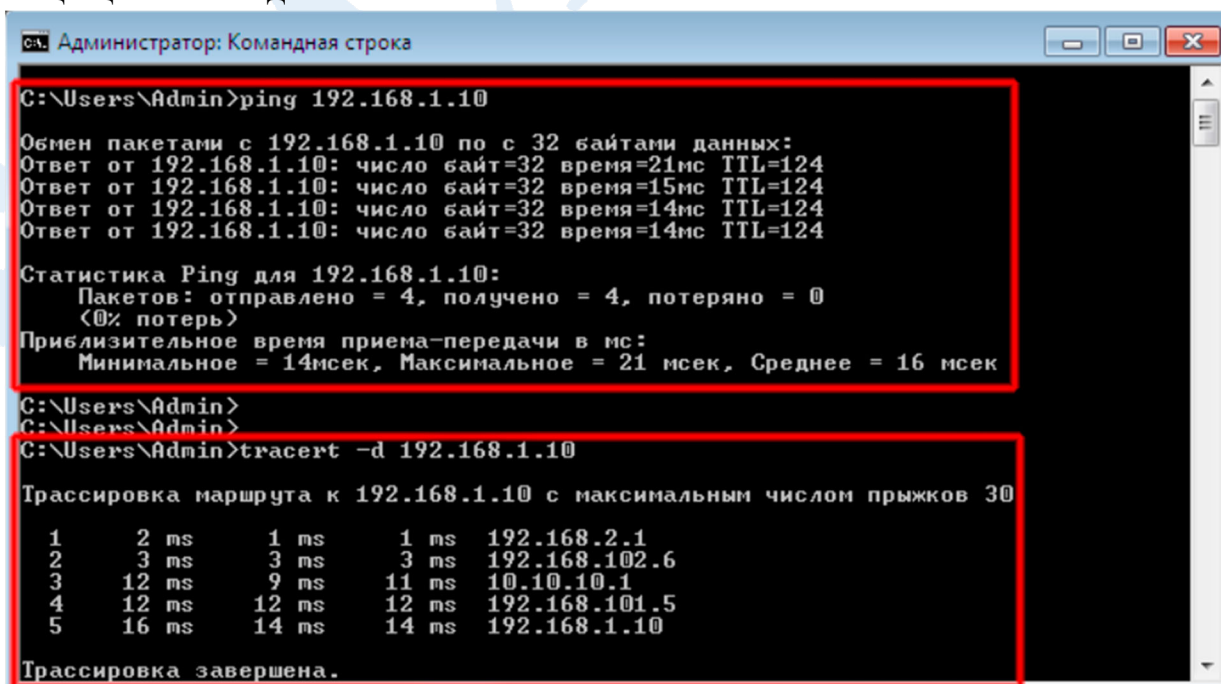
C:\Users\Admin>
C:\Users\Admin>
C:\Users\Admin>tracert -d 192.168.2.10

Трассировка маршрута к 192.168.2.10 с максимальным числом прыжков 30

 1      1 ms      1 ms      2 ms  192.168.1.1
 2      3 ms      3 ms      3 ms  192.168.101.6
 3     11 ms      9 ms      9 ms  10.10.10.2
 4     12 ms     11 ms     11 ms  192.168.102.5
 5     13 ms     12 ms     13 ms  192.168.2.10

Трассировка завершена.
```

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=14мс 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>
C:\Users\Admin>
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      3 ms      3 ms      3 ms  192.168.102.6
 3     12 ms      9 ms     11 ms  10.10.10.1
 4     12 ms     12 ms     12 ms  192.168.101.5
 5     16 ms     14 ms     14 ms  192.168.1.10

Трассировка завершена.
```