

# S-CRYPTO VPN 1.0

## Организация удаленного доступа (Remote access). Построение L2 VPN туннеля между клиентом «S-Crypto VPN Client» и шлюзом безопасности «S-Crypto VPN Server» на ОС Debian 13 находящимся за статическим NAT

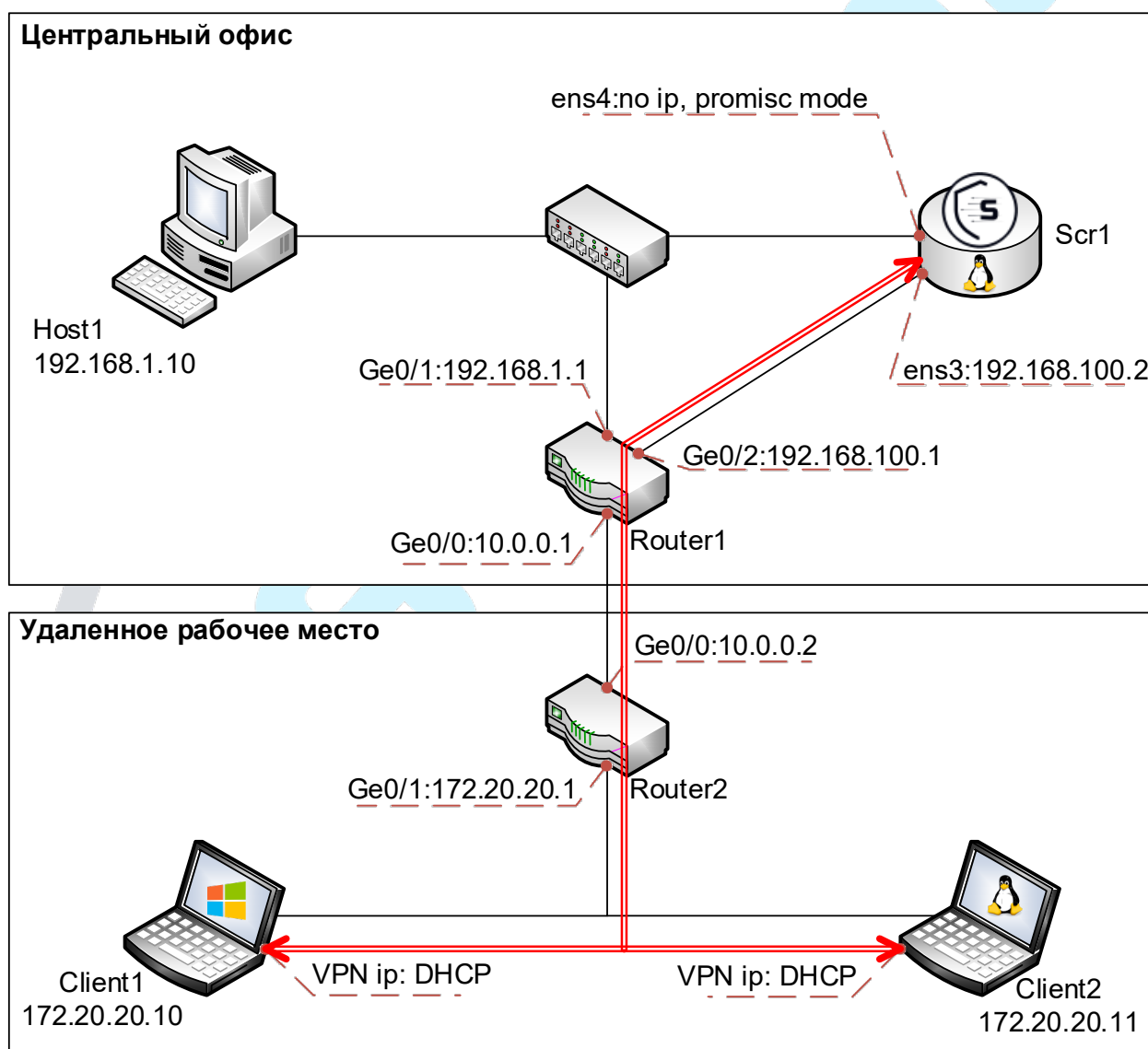
### Оглавление

1. Описание стенда .....	2
2. Описание устройства «Router1» .....	3
3. Описание устройства «Router2» .....	3
4. Описание устройства «Host1» .....	3
5. Настройка шлюза безопасности «Scr1» .....	3
6. Настройка удаленного рабочего места «Client1» на ОС Windows .....	6
7. Настройка удаленного рабочего места «Client2» на ОС Debian .....	9
8. Пример настройки правил фильтрации пакетов (Firewall) .....	10
9. Проверка работоспособности стенда .....	11
Устройство «Client1» .....	11
Устройство «Client2» .....	12
Правила фильтрации пакетов (Firewall) .....	13

## 1. Описание стенда

Сценарий содержит пример настройки сервера «S-Crypto VPN Server», установленного на операционной системе Debian 13, и клиентов «S-Crypto VPN Client», установленных на операционной системе Windows и Debian, для обеспечения безопасного доступа от удаленного рабочего места к ресурсам локальной сети центрального офиса со взаимодействием между устройствами на втором уровне модели OSI (L2).

Шлюз безопасности «S-Crypto VPN Server» центрального офиса располагается за маршрутизатором, обеспечивающим доступ в неконтролируемый сегмент (сеть Интернет) и выполняющим функции DHCP-сервера и трансляции сетевых адресов (DNAT), при этом используется статическая трансляция с пробросом назначенного администратором TCP-порта на интерфейс VPN-сервера.



## **2. Описание устройства «Router1»**

Устройство «Router1» – маршрутизатор, обеспечивающий следующие функции:

1. Доступ центрального офиса в неконтролируемый сегмент (Интернет);
2. Проброс TCP-порта 1355 (DNAT) с внешнего интерфейса маршрутизатора Ge0/0:10.0.0.1 на сетевой интерфейс VPN-сервера «Scr1» Ge0/0:192.168.100.2;
3. DHCP-сервер – присвоение ip-адресов устройствам в локальной сети центрального офиса и подключенным VPN-клиентам.

## **3. Описание устройства «Router2»**

Устройство «Router2» – маршрутизатор, обеспечивающий доступ удаленного рабочего места в неконтролируемый сегмент (Интернет).

## **4. Описание устройства «Host1»**

Устройство «Host1» – рабочее место администратора с операционной системой Windows 7 на сетевом интерфейсе которого назначен статический ip-адрес 192.168.1.10/24 gw 192.168.1.1 и установлен программный продукт «S-Crypto VPN Server Manager» для удаленного администрирования VPN-сервера «Scr1» с помощью графического пользовательского интерфейса.

## **5. Настройка шлюза безопасности «Scr1»**

Шлюз безопасности «Scr1» – устройство на базе операционной системы Debian 13 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 192.168.100.2
netmask 255.255.255.0
gateway 192.168.100.1

allow-hotplug ens4
iface ens4 inet manual
```

После внесения изменений перезапустите сетевую службу

```
sudo systemctl restart networking
```

На интерфейсе «ens3» назначен статический ip-адрес, на котором прослушивается порт TCP:1355 для администрирования сервера и терминирования входящих подключений от клиентов. Необходимость назначения ip-адреса на интерфейс «ens4» не является обязательным, т.к. интерфейс позже 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 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/>.

4. С устройства «Host1» с помощью программы «S-Crypto VPN Server Manager» подключитесь к серверу «Scr1» по ip-адресу 192.168.100.2 и создайте виртуальный хаб «Hub» для терминирования входящих подключений

Новый виртуальный хаб

Виртуальный хаба

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

Статус хаба:  
 Подключен  Отключен

Администрирование

Пароль администратора хаба:  
.....

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

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

Кластеризация

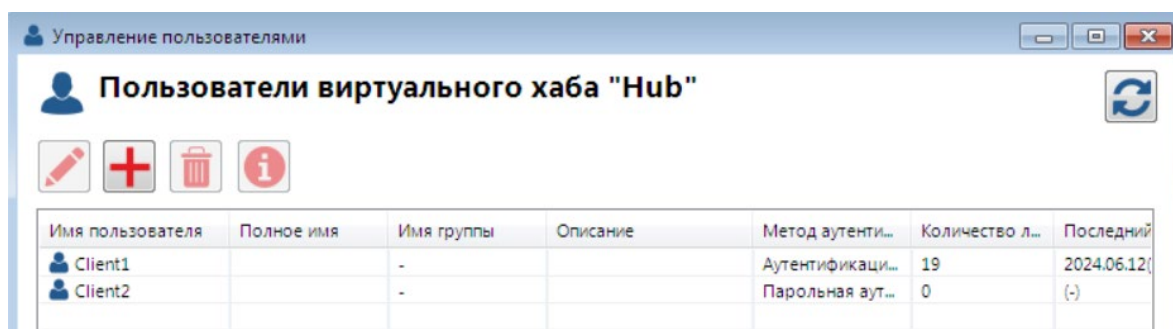
В настоящее время сервер и виртуальный хаб работают в автономном(некластерном) режиме.

Статический хаб  Динамический хаб

OK Отмена

5. В настройках созданного виртуального хаба «Hub» в разделе «Пользователи» создайте учетные записи, от имени которых будут аутентифицироваться пользователи удаленных рабочих мест Client1 и Client2. 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/>



Имя пользователя	Полное имя	Имя группы	Описание	Метод аутенти...	Количество л...	Последний
Client1		-		Аутентификаци...	19	2024.06.12(
Client2		-		Парольная аут...	0	(-)

6. В настройках сервера раздела «Локальный мост» создайте мост от виртуального хаба «Hub» к сетевому интерфейсу «ens4»



Настройка локального моста

Созданные локальные мосты

Номер	Имя виртуального хаба	Имя сетевого адаптера и...	Статус	MultiQueue
1	Hub	ens4	Онлайн	Нет

Создание нового локального моста

Виртуальный хаб: Hub

Тип моста:

- Мост с физическим сетевым адаптером
- Мост с новым TAP-устройством

Сетевой адаптер: ens4

Режим MultiQueue

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 LAN

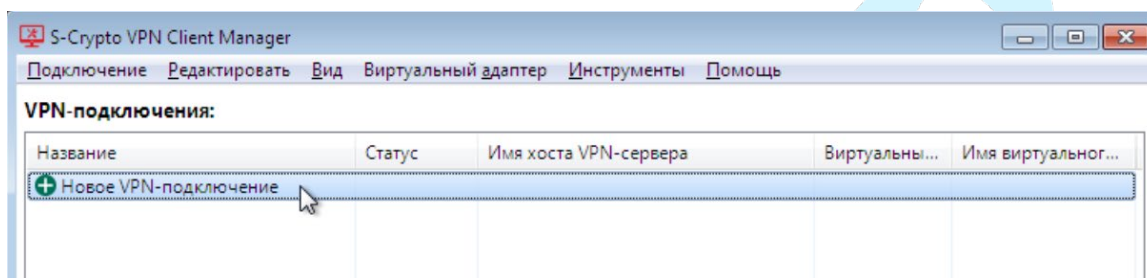
Выйти

## 6. Настройка удаленного рабочего места «Client1» на ОС Windows

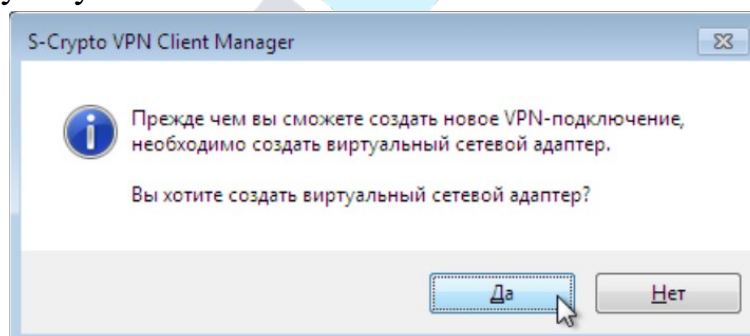
Устройство «Client1» – удаленное рабочее место на операционной системе Windows 7 x86, находящееся в неконтролируемом периметре, от которого будет устанавливаться защищенное соединение к локальной сети центрального офиса.

1. От имени учетной записи администратора произведите установку программы «S-Crypto VPN Client» и при первом запуске введите информацию о лицензии. (Информация об установке содержится в инструкции «Руководство администратора» доступной в комплекте поставки, а также на официальном сайте компании в разделе «Техническая поддержка» - «Документация» <https://s-crypto.by/support-pages/documentation/>.)

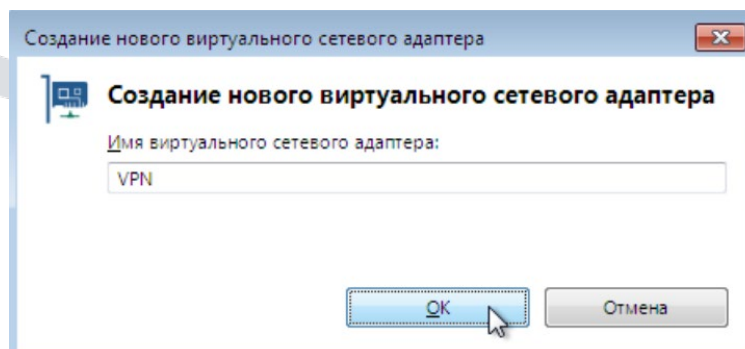
2. Создайте подключение к серверу, двойным кликом левой кнопки мыши на строке «Новое VPN-подключение»



3. Если подключение создается впервые, будет предложено создать новый виртуальный адаптер. Нажмите «Да». Если адаптер был создан ранее, переходите к пункту 6.



4. Введите название адаптера либо оставьте без изменений



5. Дождитесь создания нового адаптера. После создания адаптера, информация о нем появится в нижней части основного окна, повторно запустите процесс создания подключения (пункт 2)

**Виртуальные сетевые адаптеры:**

Имя	Статус	MAC-адрес	
VPN Client Adapter - VPN	Включен	5E-70-D1-8F-E3-43	

Не подключен S-Crypto VPN Client Manager

6. В окне «Создание нового VPN-подключения» заполните обязательные поля:

- «Название» – может иметь произвольное значение;
- «Имя хоста | IP» – внешний ip-адрес маршрутизатора «Router1»;
- «Номер TCP-порта» – порт, прослушиваемый на VPN-сервере «Scr1»;
- «Имя виртуального хаба» – название хаба на VPN-сервере «Scr1»;
- «Имя пользователя» и «пароль» – созданные на хабе VPN-сервера «Scr1».

Создание нового VPN-подключения

### Настройка VPN-соединения

Название: Тестовое подключение 1

Целевой VPN-сервер

Имя хоста | IP: 10.0.0.1

Номер TCP-порта: 1355 (SC-VPN порт)  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

Виртуальный сетевой адаптер

VPN Client Adapter - VPN

Дополнительные параметры

Настройка дополнительных параметров...

Скрыть экраны состояния и ошибок

Скрыть экраны IP-адресов

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: Client1

Пароль: .....

Изменить пароль

Настройка переподключения

Автоматическое переподключение

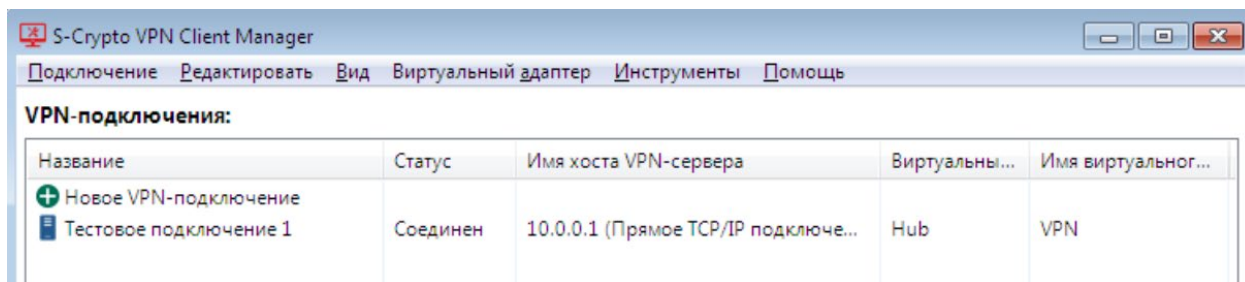
Число попыток подключений: раз

Без ограничения

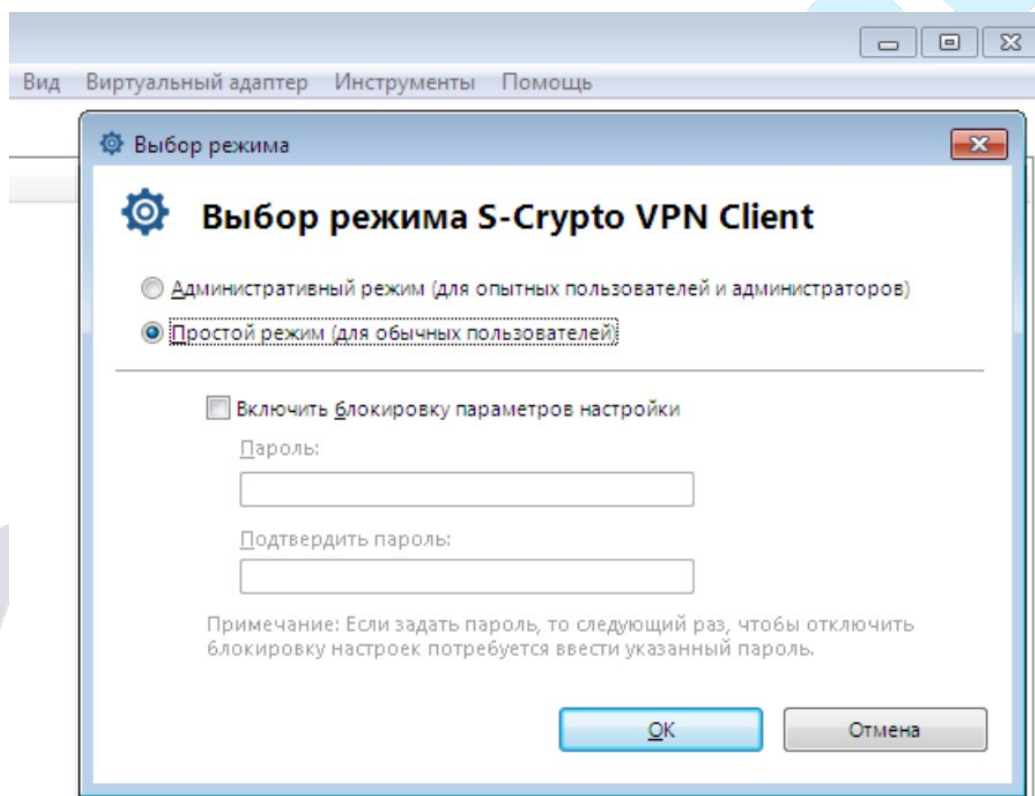
Интервал между попытками: 15 секунд

OK Отмена

7. После создания, новое подключение появится в списке подключений основного окна. Соединение с сервером можно запустить, двойным кликом левой кнопки мыши на нем.



8. Вид основного окна можно переключить в «пользовательский режим», для скрытия административных параметров. Для этого необходимо нажать «Вид» - «Выбор режима» - «Простой». Если при этом установить пароль, то доступ для изменения настроек будет ограничен.



## 7. Настройка удаленного рабочего места «Client2» на ОС Debian

Устройство «Client2» – удаленное рабочее место на операционной системе Debian, находящееся в неконтролируемом периметре, от которого будет устанавливаться защищенное соединение к локальной сети центрального офиса.

1. От имени учетной записи root произведите установку программы «S-Crypto VPN Client»

```
dpkg -i /opt/scrypto-vpnclient-v1.0.0-linux-x86_64.deb
```

2. Запустите утилиту управления, выбрать пункт 2 и на предложение о вводе ip-адреса нажмите «Enter»

```
vpnclient  
2
```

3. Введите информацию о лицензии (если не была добавлена ранее)

```
LicenseAdd NCI7OG-*****-*****-*****-*****-*****
```

4. Создайте виртуальный адаптер

```
NicCreate VPN
```

5. Создайте новое подключение к виртуальному хабу «Hub», VPN-сервера «Scr1»

```
AccountCreate TestConnect1 /SERVER:10.0.0.1:1355 /HUB:Hub /USERNAME:Client2  
/NICNAME:VPN
```

6. Установите способ аутентификации (в примере используется аутентификация по паролю)

```
AccountPasswordSet TestConnect1 /PASSWORD:passwd123 /TYPE:standard
```

7. Установите автозапуск VPN-подключения при старте клиента

```
AccountStartupSet TestConnect1
```

8. Добавьте описание виртуального интерфейса «VPN» в файл /etc/network/interfaces для получения ip-адреса от DHCP-сервера после установки VPN-соединения

```
allow-hotplug vpn_vpn  
iface vpn_vpn inet dhcp
```

9. Перезагрузите компьютер

```
reboot
```

Примечание

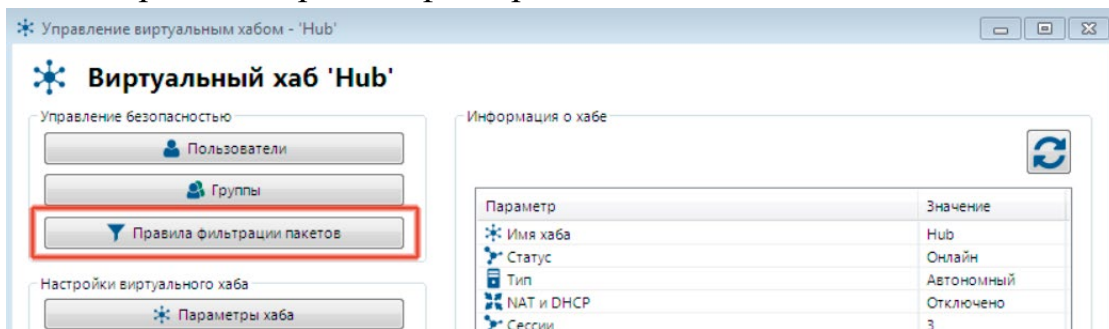
Команда для запуска службы клиента: `vpnclient start`

Команда для остановки службы клиента: `vpnclient stop`

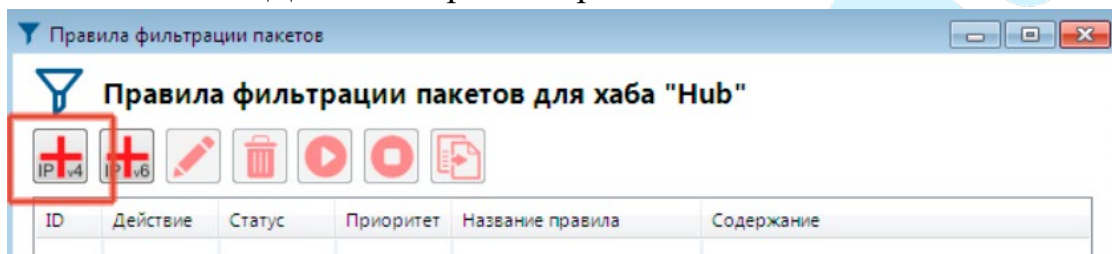
## 8. Пример настройки правил фильтрации пакетов (Firewall)

В качестве примера повышения безопасности сети запретим возможность доступа всех удаленных клиентов к основному маршрутизатору центрального офиса «Router1» по его ip-адресу «192.168.1.1»

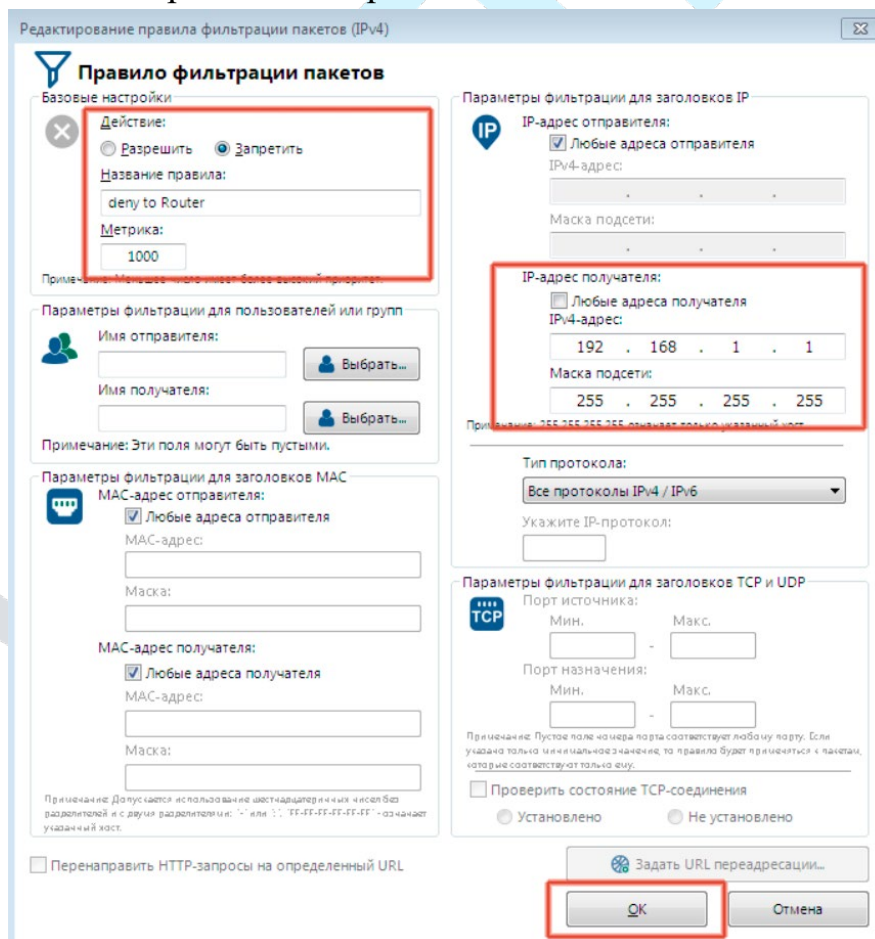
1. В настройках созданного виртуального хаба «Hub» сервера «Scr1» перейдите в раздел «Правила фильтрации пакетов»



2. Нажмите «Добавить правило ipv4»



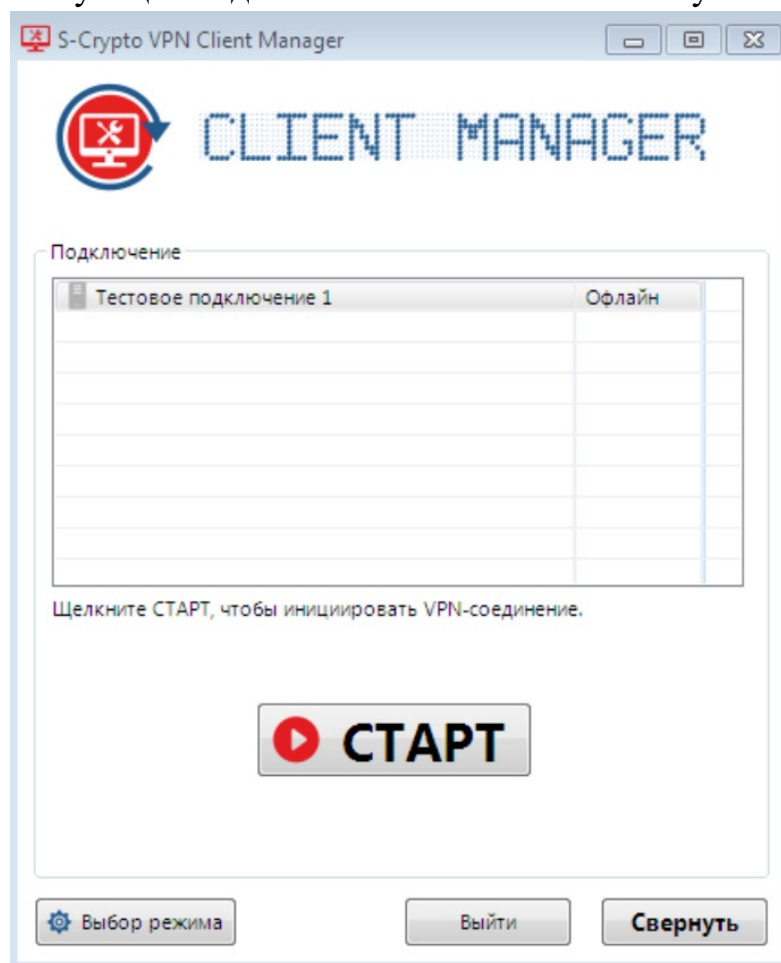
3. Внесите запрещающее правило и нажмите «ОК»



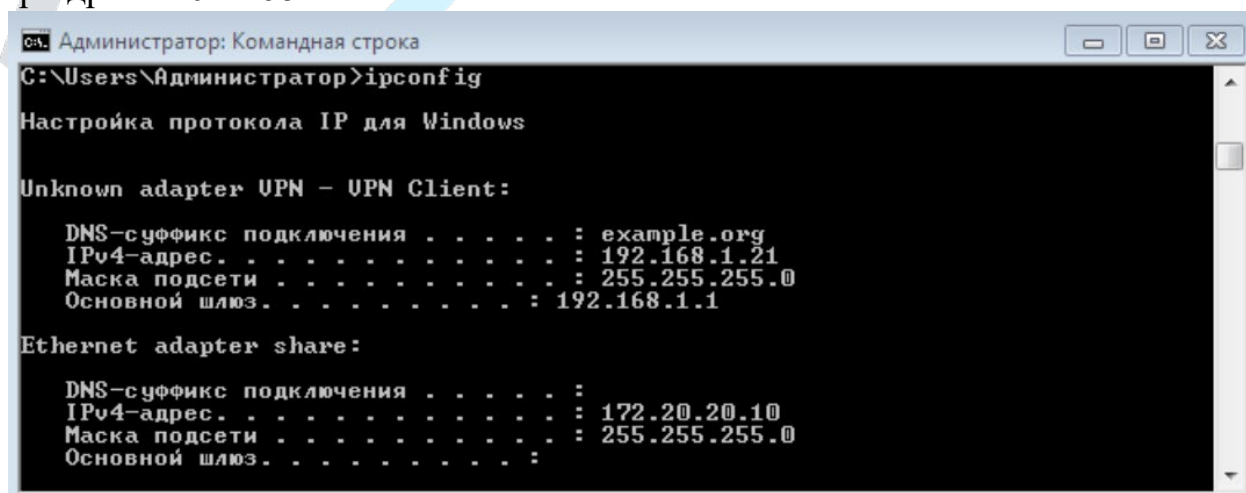
## 9. Проверка работоспособности стенда

### Устройство «Client1»

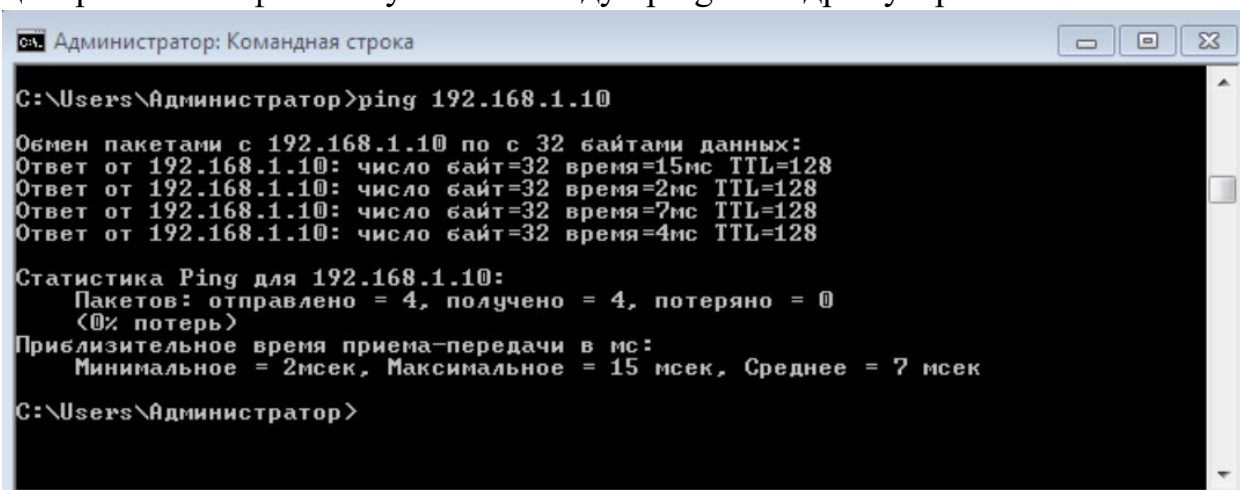
1. На устройстве «Client1» установим соединение с сервером «Scr1» выбрав соответствующее подключение и нажав на кнопку «Старт»



2. Откроем «командную строку» и введя команду «ipconfig», убедимся, что виртуальный адаптер получил ip-адрес от dhcp-сервера на устройстве «Router1». На скриншоте ниже видно, что при подключении был получен ip-адрес – 192.168.1.21



3. Проверим доступность сетевых устройств в локальной сети центрального офиса запустив команду «ping» на адрес устройства «Host1»



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

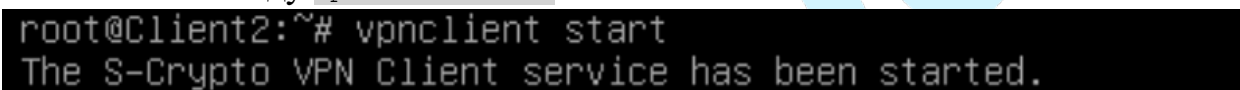
Обмен пакетами с 192.168.1.10 по с 32 байтами данных:
Ответ от 192.168.1.10: число байт=32 время=15мс TTL=128
Ответ от 192.168.1.10: число байт=32 время=2мс TTL=128
Ответ от 192.168.1.10: число байт=32 время=7мс TTL=128
Ответ от 192.168.1.10: число байт=32 время=4мс TTL=128

Статистика Ping для 192.168.1.10:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
    Приблизительное время приема-передачи в мс:
    Минимальное = 2мсек, Максимальное = 15 мсек, Среднее = 7 мсек

C:\Users\Администратор>
```

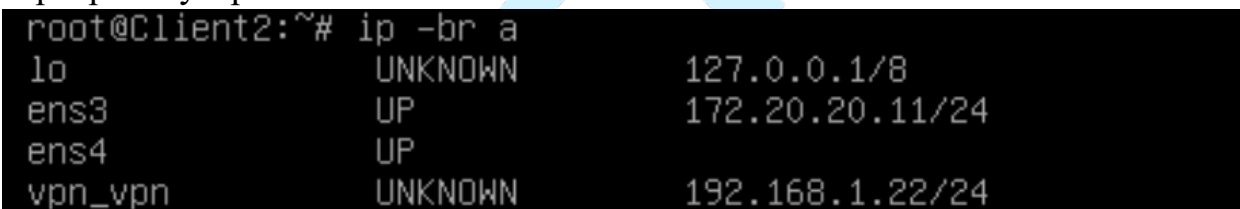
## Устройство «Client2»

1. На устройстве «Client2» установим соединение с сервером «Scr1»  
ВЫПОЛНИВ КОМАНДУ `vpnclient start`



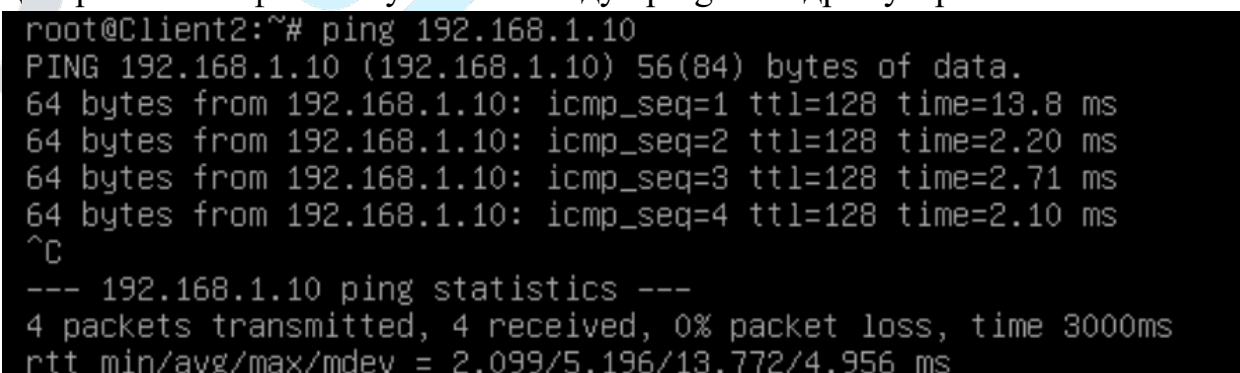
```
root@Client2:~# vpnclient start
The S-Crypto VPN Client service has been started.
```

2. Убедимся, что виртуальный адаптер получил ip-адрес от dhcp-сервера на устройстве «Router1»



```
root@Client2:~# ip -br a
lo                UNKNOWN          127.0.0.1/8
ens3              UP               172.20.20.11/24
ens4              UP
vpn_vpn           UNKNOWN          192.168.1.22/24
```

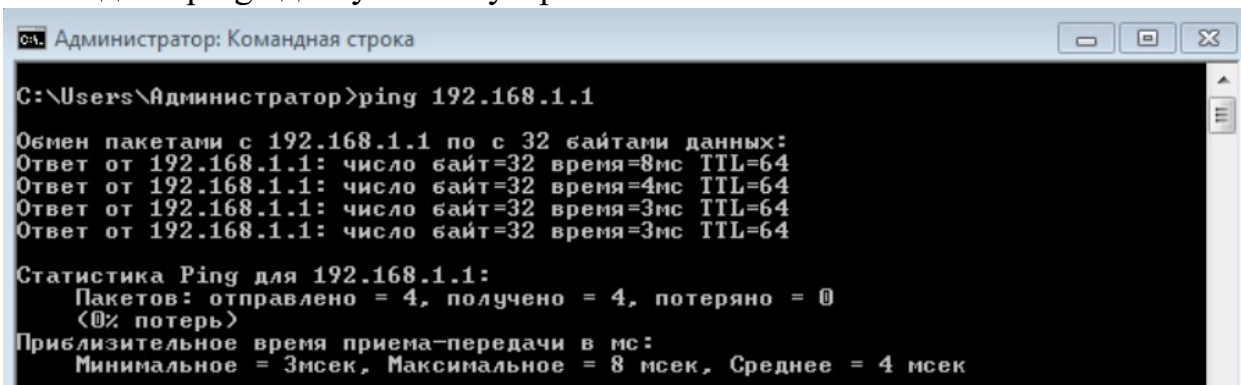
3. Проверим доступность сетевых устройств в локальной сети центрального офиса запустив команду «ping» на адрес устройства «Host1»



```
root@Client2:~# ping 192.168.1.10
PING 192.168.1.10 (192.168.1.10) 56(84) bytes of data.
64 bytes from 192.168.1.10: icmp_seq=1 ttl=128 time=13.8 ms
64 bytes from 192.168.1.10: icmp_seq=2 ttl=128 time=2.20 ms
64 bytes from 192.168.1.10: icmp_seq=3 ttl=128 time=2.71 ms
64 bytes from 192.168.1.10: icmp_seq=4 ttl=128 time=2.10 ms
^C
--- 192.168.1.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3000ms
rtt min/avg/max/mdev = 2.099/5.196/13.772/4.956 ms
```

## Правила фильтрации пакетов (Firewall)

1. После установки соединения с устройства «Client1» проверим командой «ping» доступность устройства «Router1»



```
Администратор: Командная строка

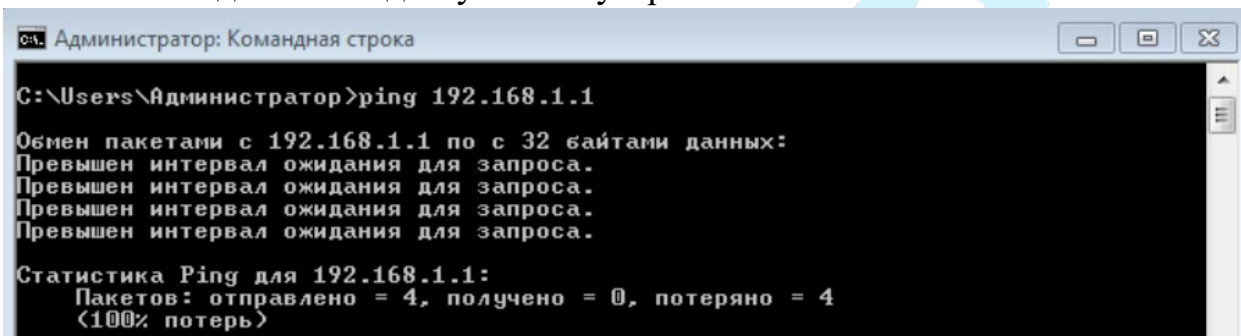
C:\Users\Администратор>ping 192.168.1.1

Обмен пакетами с 192.168.1.1 по с 32 байтами данных:
Ответ от 192.168.1.1: число байт=32 время=8мс TTL=64
Ответ от 192.168.1.1: число байт=32 время=4мс TTL=64
Ответ от 192.168.1.1: число байт=32 время=3мс TTL=64
Ответ от 192.168.1.1: число байт=32 время=3мс TTL=64

Статистика Ping для 192.168.1.1:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (<0% потерь>)
    Приблизительное время приема-передачи в мс:
    Минимальное = 3мсек, Максимальное = 8 мсек, Среднее = 4 мсек
```

2. Применим правило, описанное в п.8 инструкции

3. Убедимся в недоступности устройства «Router1»



```
Администратор: Командная строка

C:\Users\Администратор>ping 192.168.1.1

Обмен пакетами с 192.168.1.1 по с 32 байтами данных:
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.

Статистика Ping для 192.168.1.1:
    Пакетов: отправлено = 4, получено = 0, потеряно = 4
    (<100% потерь>)
```