

S-CRYPTO VPN 1.0

**Организация удаленного доступа (Remote access).
Построение VPN туннеля между шлюзом безопасности «S-Crypto VPN Server» на ОС Windows, находящимся за статическим NAT, и клиентом «S-Crypto VPN Client» с получением адреса от DHCP-сервера и использованием функции виртуального NAT для доступа в локальную сеть**

Сценарий описывает возможности программного продукта «S-Crypto VPN Server» в использовании интегрированной функции виртуального NAT. Сценарий не рекомендуется к использованию в высокопроизводительных сценариях в связи с её невысокой пропускной способностью. При проектировании сети рекомендуется воспользоваться иными сценариями, без использования вышеуказанной функции.

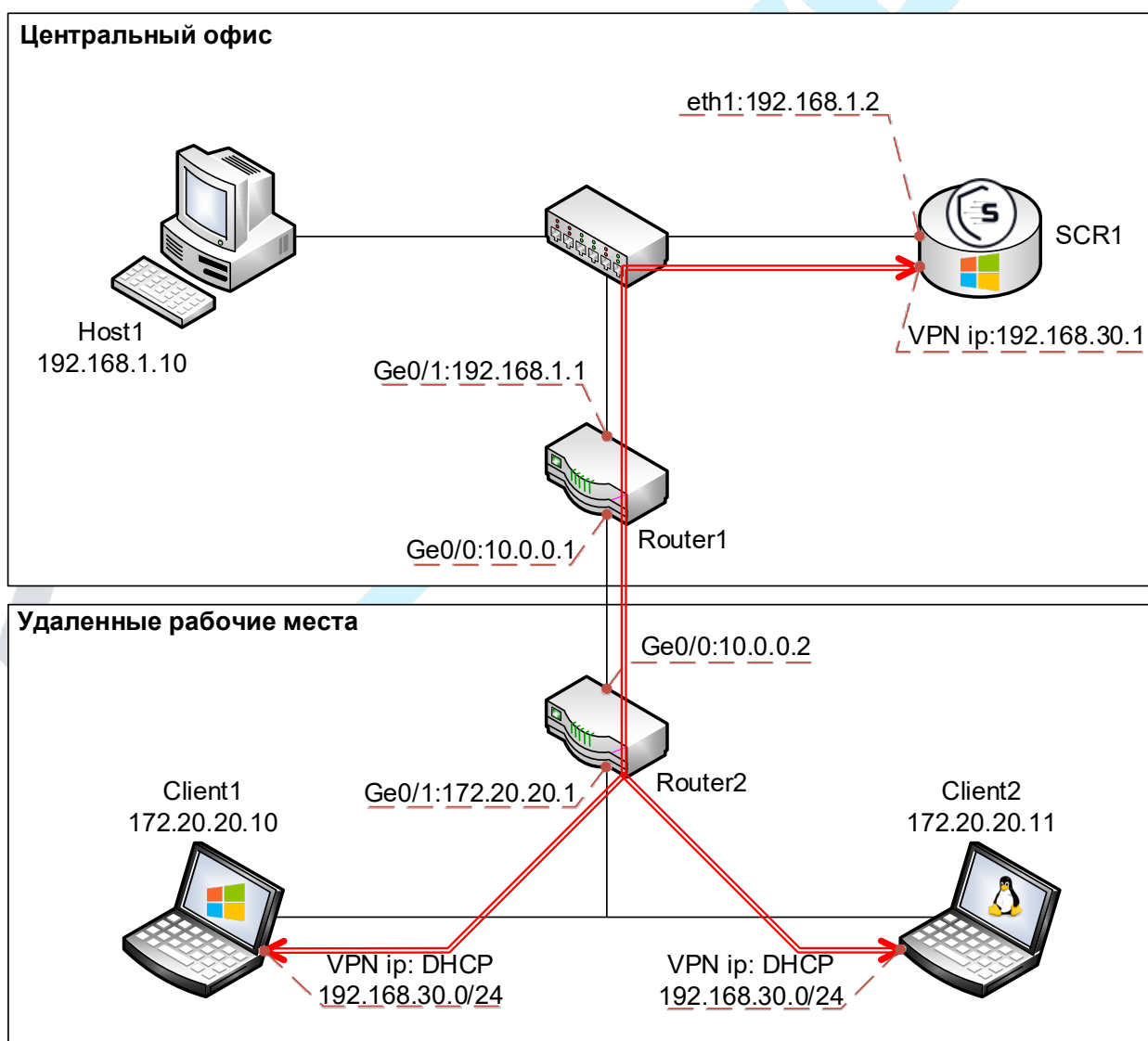
Оглавление

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.....	8
7. Настройка удаленного рабочего места «Client2» на ОС Debian	11
8. Пример настройки правил фильтрации пакетов (Firewall)	12
9. Проверка работоспособности стенда.....	13
Устройство «Client1»	13
Устройство «Client2»	15
Правила фильтрации пакетов (Firewall).....	16

1. Описание стенда

Сценарий содержит пример настройки сервера «S-Crypto VPN Server», установленного на операционной системе Windows, и клиентов «S-Crypto VPN Client», установленных на операционных системах Windows и Debian, для обеспечения безопасного доступа от удаленных рабочих мест к ресурсам локальной сети центрального офиса. При подключении клиентов к VPN-серверу производится выдача ip-адреса и статических маршрутов от интегрированного DHCP-сервера. Доступ клиентов в локальную сеть осуществляется с использованием встроенной функции виртуального NAT с ip-адреса VPN-сервера.

Шлюз безопасности «S-Crypto VPN Server» центрального офиса располагается за маршрутизатором «Router1», обеспечивающим доступ в неконтролируемый сегмент (сеть Интернет) и функцию 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» Ge0/0:192.168.1.2;

3. Описание устройства «Router2»

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

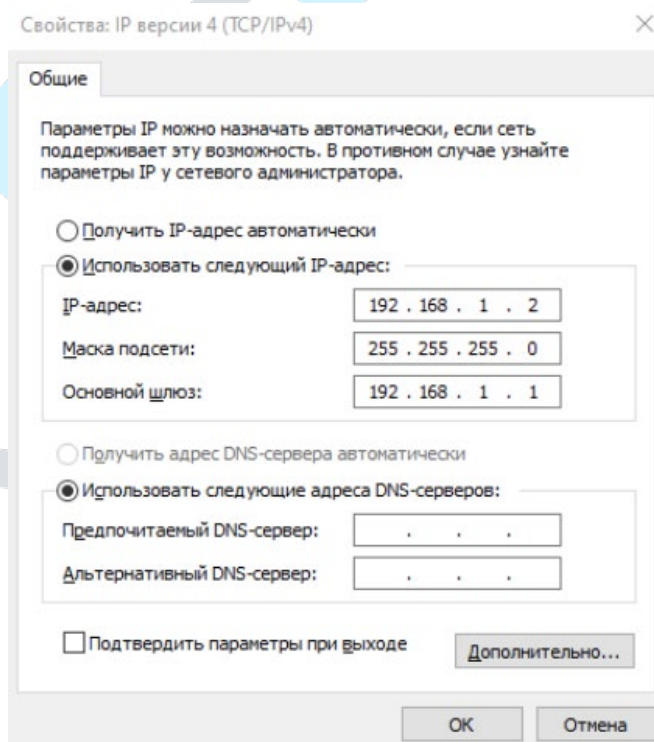
4. Описание устройства «Host1»

Устройство «Host1» – сетевое устройство с назначенным статическим ip-адресом 192.168.1.10/24 gw 192.168.1.1. Используется в сценарии для тестирования доступности устройств в локальной сети центрального офиса.

5. 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 «Ethernet»



2. 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/>.

3. 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

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

Управление виртуальным хабом - 'Hub'

Виртуальный хаб 'Hub'

Управление безопасностью

Пользователи

Группы

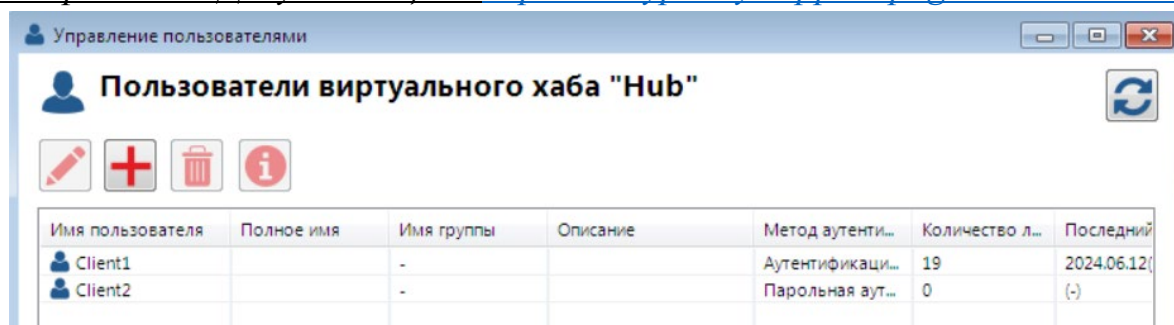
Правила фильтрации пакетов

Информация о хаб

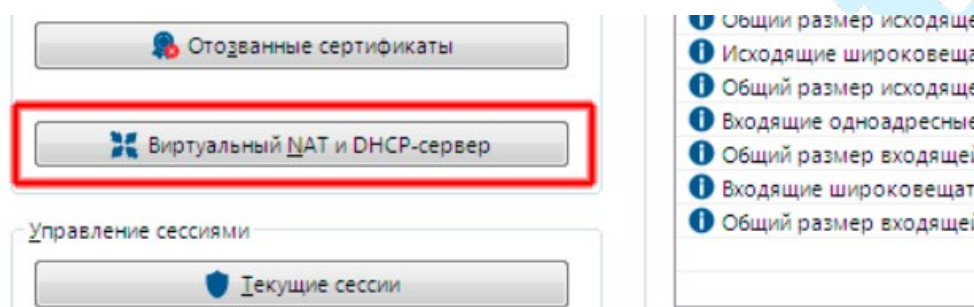
Параметр
Имя хаба
Статус

5. Создайте учетные записи, от имени которых будут аутентифицироваться пользователи удаленных рабочих мест Client1 и Client2.
Информация о настройке различных способов аутентификации

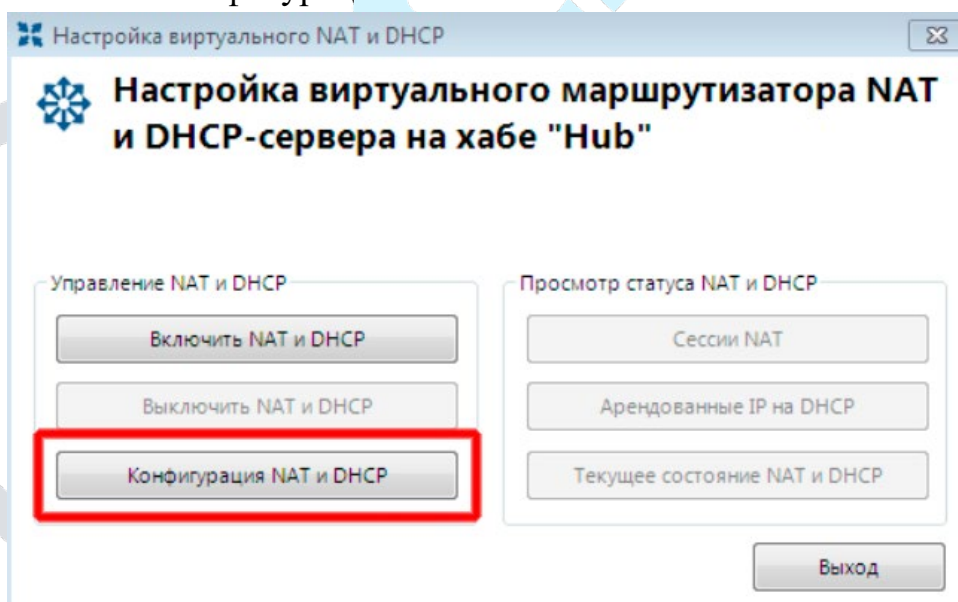
пользователей размещена в инструкции «Способы аутентификации» доступной на официальном сайте компании в разделе «Техническая поддержка» - «Документация» <https://s-crypto.by/support-pages/documentation/>



6. В настройках созданного виртуального хаба «Hub» откройте раздел «Виртуальный NAT и DHCP-сервер»



7. Нажмите конфигурация NAT и DHCP



8. Настройте виртуальный маршрутизатор по примеру со скриншотом

Конфигурация виртуального NAT и DHCP

Конфигурация виртуального NAT и DHCP на хабе "Hub"

Настройки сетевого интерфейса виртуального хоста

MAC-адрес: 5E-87-B3-12-23-9A

IP-адрес: 192 . 168 . 30 . 1

Маска подсети: 255 . 255 . 255 . 0

Настройки виртуального DHCP-сервера

Использовать функции виртуального DHCP-сервера

Начальный IP-адрес: 192 . 168 . 30 . 10

Конечный IP-адрес: 192 . 168 . 30 . 200

Маска подсети: 255 . 255 . 255 . 0

Срок аренды: 7200 секунд

Настройки виртуального NAT

Использовать функции виртуального NAT

Значение MTU: 1500 байт

Тайм-аут сеанса TCP: 1800 секунд

Тайм-аут сеанса UDP: 60 секунд

Таблица статической маршрутизации

Таблица статической маршрутизации отправляемая VPN-клиентам (для раздельного туннелирования):

Отредактировать таблицу статической маршрутизации

Параметры, применяемые к DHCP-клиентам (необязательно)

Шлюз по умолчанию: . . .

Предпочитаемый DNS-сервер: 192 . 168 . 1 . 1

Альтернативный DNS-сервер: . . .

Домен по умолчанию:

Сохранить операции NAT и DHCP-сервера в журнале событий

OK Отмена

9. Настройте маршрутизацию трафика от клиентов одним из вариантов:
- Если предполагается, что весь трафик со стороны клиента должен попадать в защищенный туннель в том числе и доступ в Интернет, тогда укажите адрес шлюза по-умолчанию

Параметры, применяемые к DHCP-клиентам (необязательно)

Шлюз по умолчанию: 192 . 168 . 30 . 1

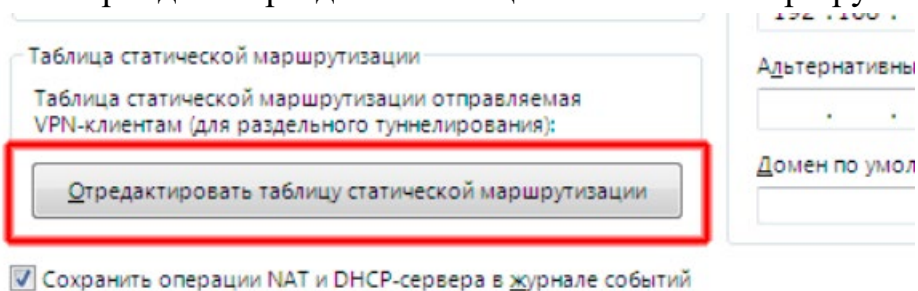
Предпочитаемый DNS-сервер: 192 . 168 . 1 . 1

Альтернативный DNS-сервер: . . .

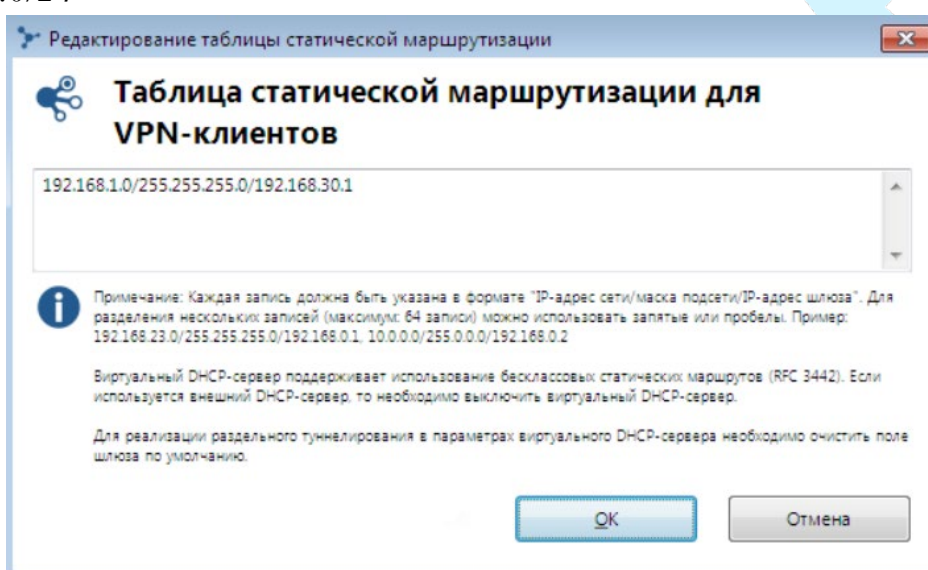
Домен по умолчанию:

- Если предполагается, что в защищенный туннель должен попадать только трафик, предназначенный для доступа к устройствам, находящимся в

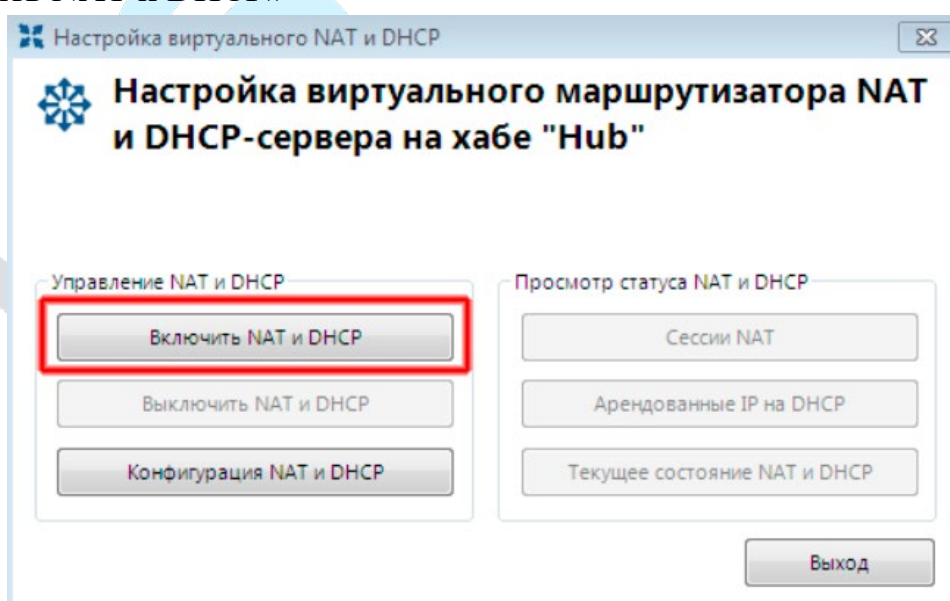
локальной подсети/подсетях, тогда поле «Шлюз по умолчанию» оставьте пустым, затем перейдите в раздел «Таблица статической маршрутизации»



И настройте статические маршруты, которые будут переданы подключенным клиентам. На скриншоте указано, что в защищенный туннель со стороны клиента будет передаваться только трафик, предназначенный для подсети 192.168.1.0/24



10. Нажатием кнопок «ОК» примените настройки и закройте открытые окна. Вернувшись к окну «Настройка виртуального NAT и DHCP» нажмите «Включить NAT и DHCP»

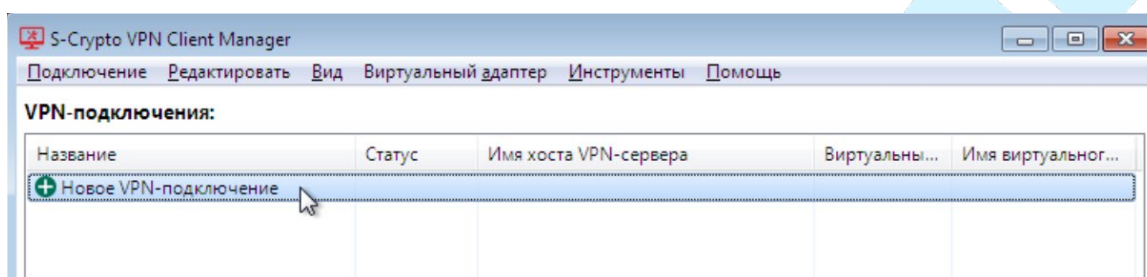


6. Настройка удаленного рабочего места «Client1» на ОС Windows

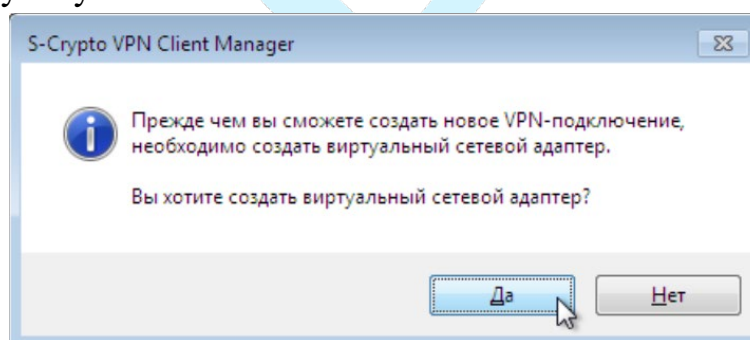
Устройство «Client1» – удаленное рабочее место на операционной системе Windows 7 x86, находящееся в неконтролируемом периметре, от которого будет устанавливаться защищенное соединение к локальной сети центрального офиса.

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/>.)

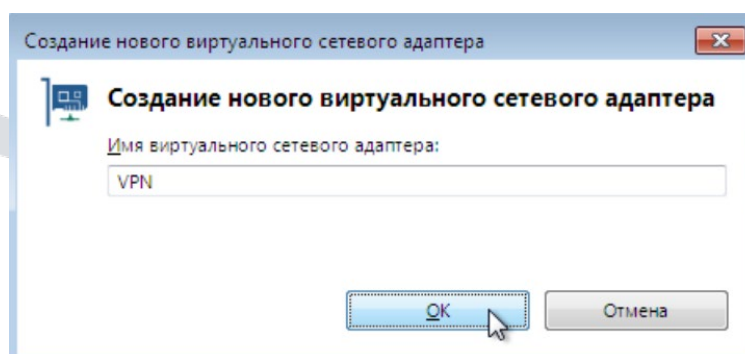
2. Создайте подключение к серверу, двойным кликом левой кнопки мыши на строке «Новое VPN-подключение»



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.

6. 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

7. 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

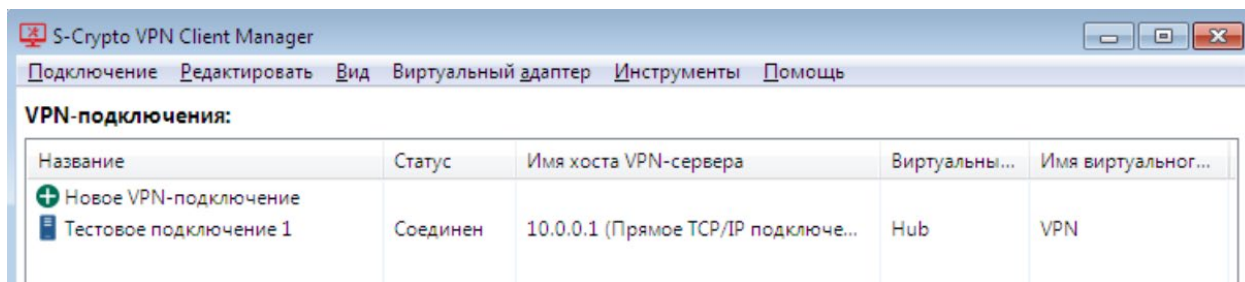
Число попыток подключений: раз

Без ограничения

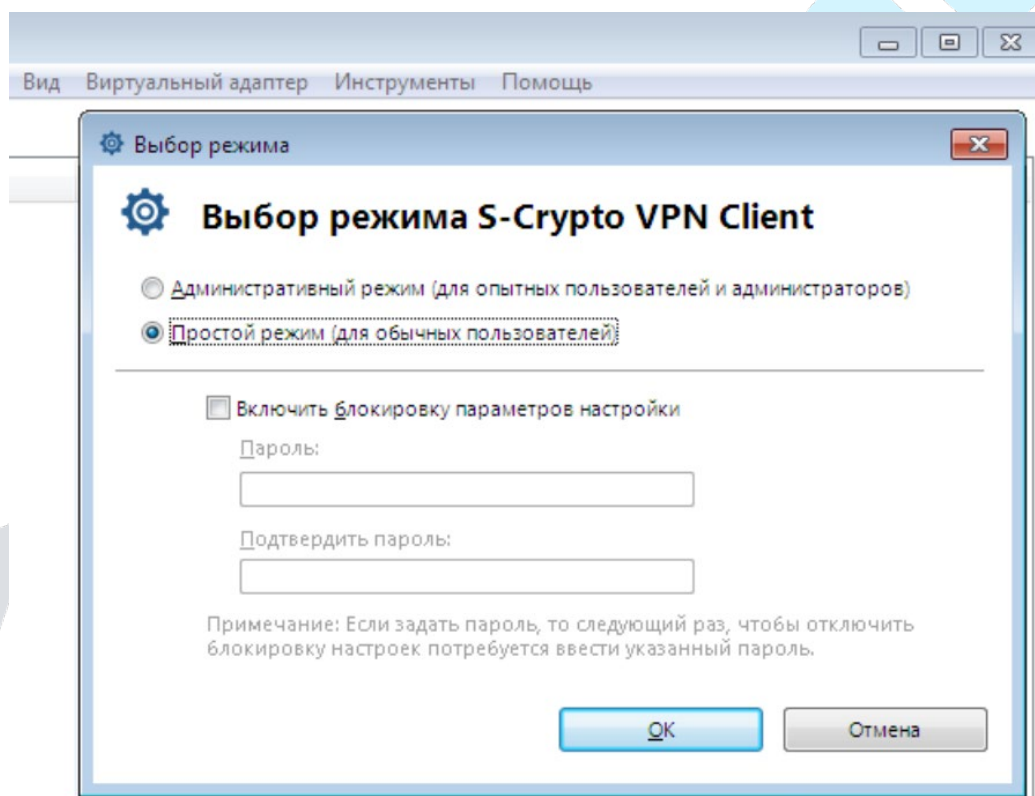
Интервал между попытками: 15 секунд

OK Отмена

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



9. 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

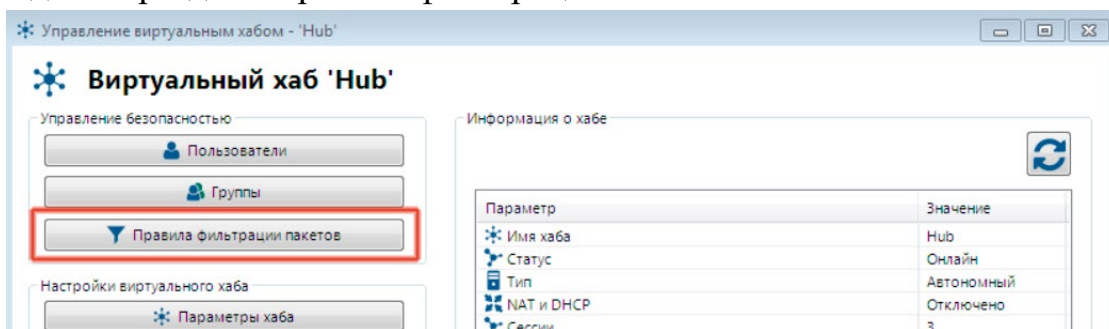
Команда для запуска службы клиента: `vpnclient start`

Команда для остановки службы клиента: `vpnclient stop`

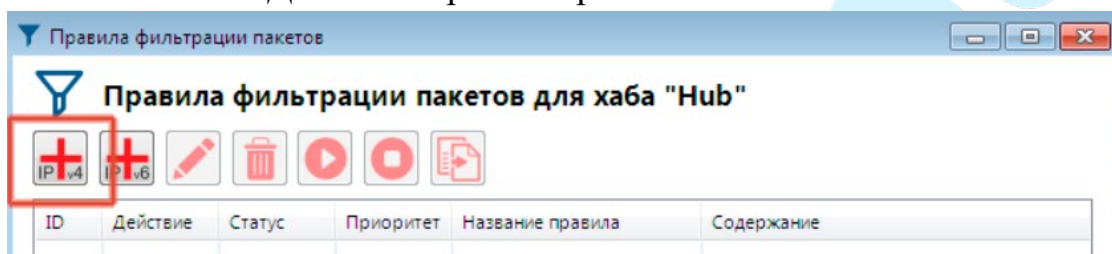
8. Пример настройки правил фильтрации пакетов (Firewall)

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»

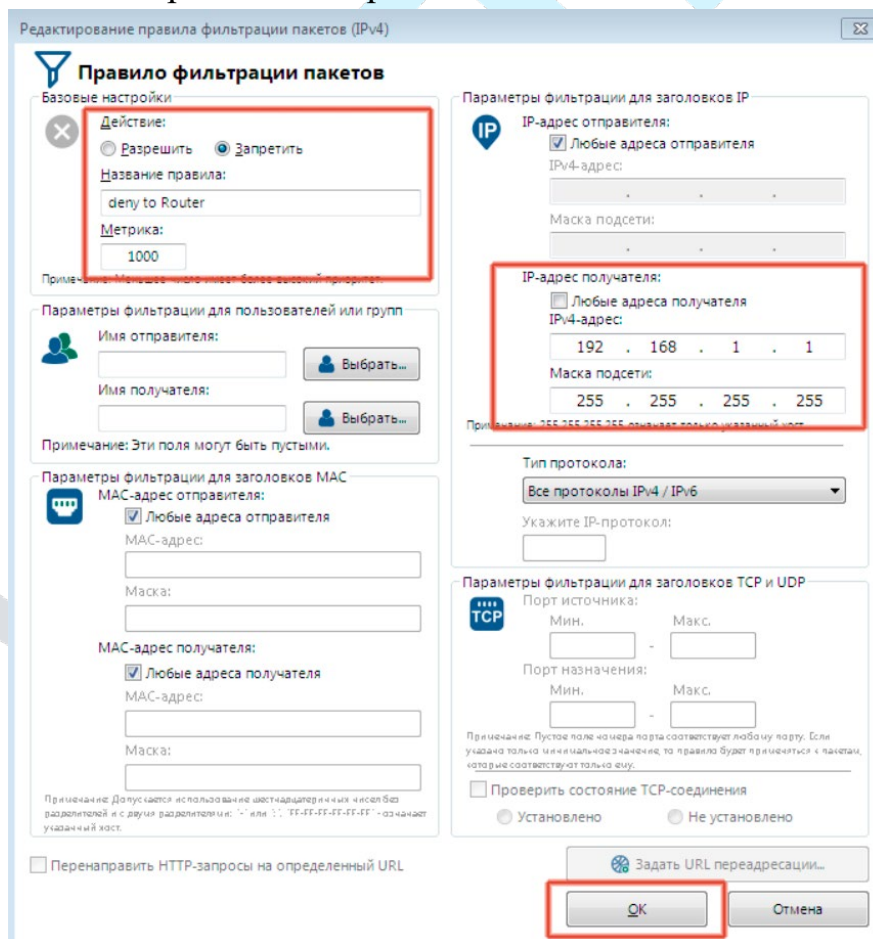
1. В настройках созданного виртуального хаба «Hub» сервера «Scr1» перейдите в раздел «Правила фильтрации пакетов»



2. Нажмите «Добавить правило ipv4»



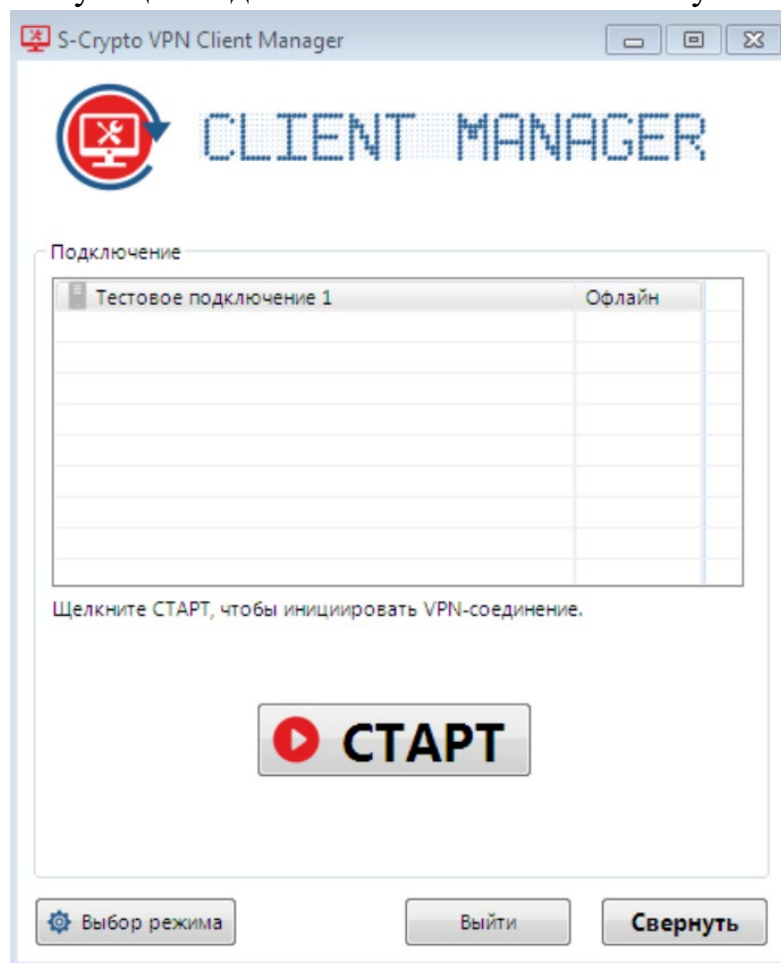
3. Внесите запрещающее правило и нажмите «ОК»



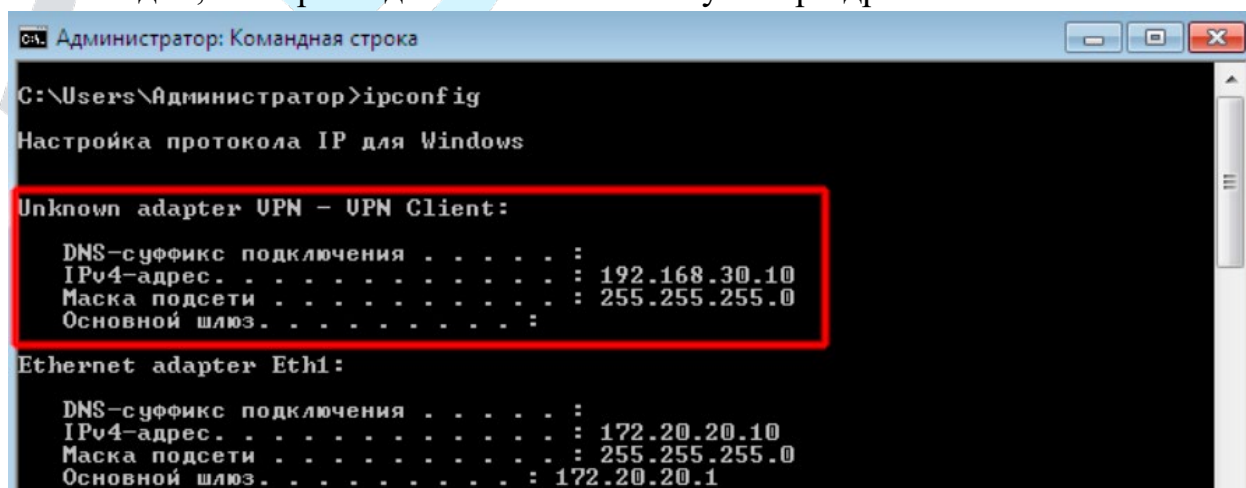
9. Проверка работоспособности стенда

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 скриншоте ниже видно, что при подключении был получен ip-адрес – 192.168.30.10



3. Убедимся в получении маршрутной информации введя команду «route print»

```
Администратор: Командная строка
C:\Users\Администратор>route print
=====
Список интерфейсов
16...5e 70 d1 8f e3 43 .....UPN Client Adapter - UPN
11...50 0e 00 02 00 00 .....Сетевое подключение Intel(R) PRO/1000 MT
1.....Software Loopback Interface 1
12...00 00 00 00 00 00 e0 Адаптер Microsoft ISATAP
13...00 00 00 00 00 00 e0 Адаптер Microsoft ISATAP
=====

IPv4 таблица маршрута
=====
Активные маршруты:
Сетевой адрес      Маска сети      Адрес шлюза      Интерфейс      Метрика
0.0.0.0            0.0.0.0        172.20.20.1      172.20.20.10   956
10.0.0.1          255.255.255.255 172.20.20.1      172.20.20.10   956
127.0.0.0         255.0.0.0      On-link          127.0.0.1      306
127.0.0.1         255.255.255.255 On-link          127.0.0.1      306
127.255.255.255   255.255.255.255 On-link          127.0.0.1      306
172.20.20.0       255.255.255.0  On-link          172.20.20.10   956
172.20.20.10     255.255.255.255 On-link          172.20.20.10   956
172.20.20.255    255.255.255.255 On-link          172.20.20.10   956
192.168.1.0       255.255.255.0  192.168.30.1     192.168.30.10   2
192.168.30.0     255.255.255.0  On-link          192.168.30.10  257
192.168.30.10    255.255.255.255 On-link          192.168.30.10  257
192.168.30.255   255.255.255.255 On-link          192.168.30.10  257
224.0.0.0        240.0.0.0      On-link          127.0.0.1      306
224.0.0.0        240.0.0.0      On-link          172.20.20.10   956
224.0.0.0        240.0.0.0      On-link          192.168.30.10  257
255.255.255.255   255.255.255.255 On-link          127.0.0.1      306
255.255.255.255   255.255.255.255 On-link          172.20.20.10   956
255.255.255.255   255.255.255.255 On-link          192.168.30.10  257
=====

Постоянные маршруты:
Сетевой адрес      Маска      Адрес шлюза      Метрика
0.0.0.0            0.0.0.0      172.20.20.1     По умолчанию
=====
```

4. 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=6мс TTL=127
Ответ от 192.168.1.10: число байт=32 время=6мс TTL=127
Ответ от 192.168.1.10: число байт=32 время=4мс TTL=127
Ответ от 192.168.1.10: число байт=32 время=4мс TTL=127

Статистика Ping для 192.168.1.10:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (<0% потерь>)
    Приблизительное время приема-передачи в мс:
    Минимальное = 4мсек, Максимальное = 6 мсек, Среднее = 5 мсек
```

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          192.168.30.11/24
root@Client2:~#
```

3. Убедимся в получении маршрутной информации

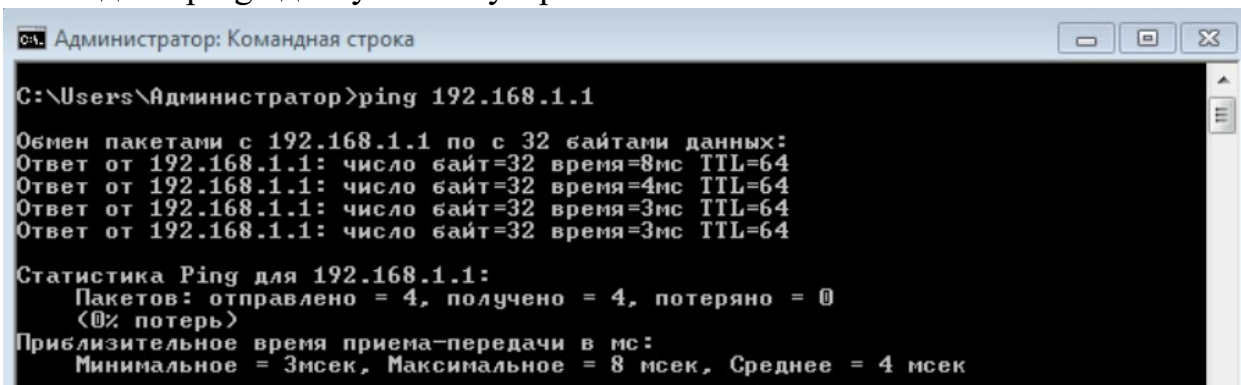
```
root@Client2:~# ip route
default via 172.20.20.1 dev ens3 onlink
172.20.20.0/24 dev ens3 proto kernel scope link src 172.20.20.11
192.168.1.0/24 via 192.168.30.1 dev vpn_vpn
192.168.30.0/24 dev vpn_vpn proto kernel scope link src 192.168.30.11
root@Client2:~#
```

4. 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=127 time=6.77 ms
64 bytes from 192.168.1.10: icmp_seq=2 ttl=127 time=2.43 ms
64 bytes from 192.168.1.10: icmp_seq=3 ttl=127 time=3.48 ms
64 bytes from 192.168.1.10: icmp_seq=4 ttl=127 time=3.36 ms
64 bytes from 192.168.1.10: icmp_seq=5 ttl=127 time=5.18 ms
64 bytes from 192.168.1.10: icmp_seq=6 ttl=127 time=5.98 ms
^C
--- 192.168.1.10 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5007ms
rtt min/avg/max/mdev = 2.426/4.530/6.766/1.550 ms
```

Правила фильтрации пакетов (Firewall)

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



```
Администратор: Командная строка

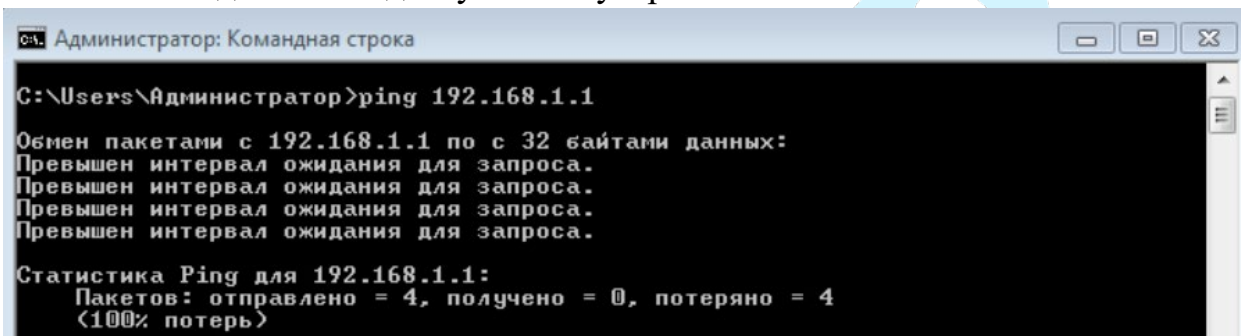
C:\Users\Администратор>ping 192.168.1.1

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 разделе 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>)
```