

S-CRYPTO VPN 1.0

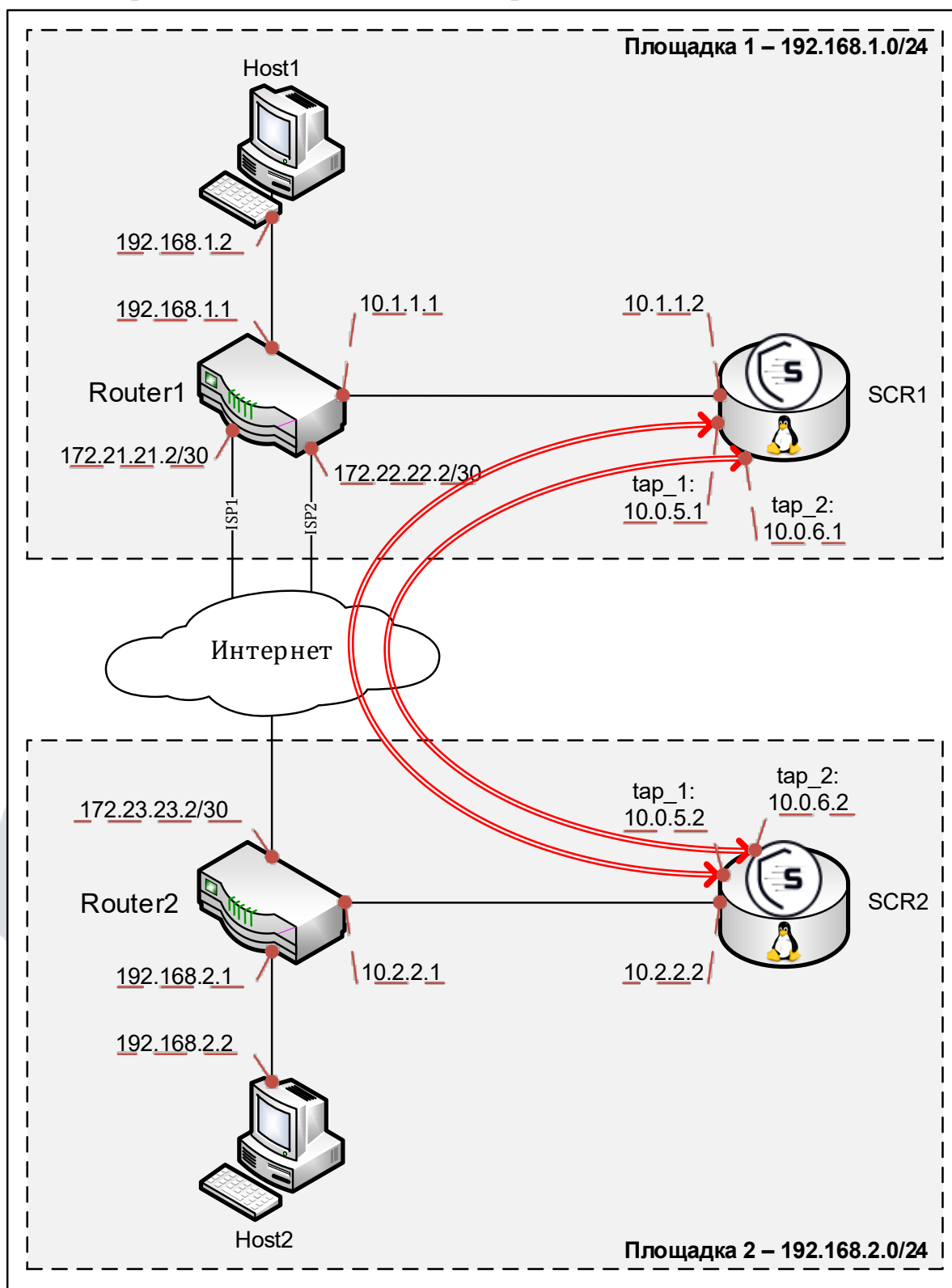
Построение отказоустойчивого решения при наличии резервного провайдера в центральном узле с выбором активного канала передачи данных с помощью скрипта

Оглавление

1. Описание стенда	2
2. Логика работы	3
3. Описание устройства «Router1»	3
4. Описание устройства «Router2»	3
5. Описание устройства «Host1»	3
6. Описание устройства «Host2»	4
7. Описание устройства «SCR1»	4
7.1 Настройка операционной системы	4
7.2 Создание скрипта и настройка его запуска.....	4
7.3 Настройка «S-Crypto VPN Server»	6
8. Описание устройства «SCR2»	7
8.1 Настройка операционной системы	7
8.2 Создание скрипта и настройка его запуска.....	8
8.3 Настройка «S-Crypto VPN Server»	9

1. Описание стенда

Сценарий содержит пример построения отказоустойчивого безопасного взаимодействия между двумя удаленными площадками. Отказоустойчивость центральной площадки достигается за счет построения между площадками двух защищенных соединений через двух различных провайдеров. Передача пользовательского трафика происходит через одно соединение. В случае отключения основного провайдера переключение на резервный канал происходит с помощью периодически выполняемого скрипта.



2. Логика работы

В рамках сценария резервируются провайдеры (каналы связи). Это достигается за счет построения двух VPN-туннелей от удаленной площадки к центральной через двух провайдеров. Для обеспечения одновременного обслуживания двух подключений, на каждом VPN-сервере будут созданы по два виртуальных хаба. Внутри туннелей пропускается полезный трафик, который будет проходить через основной ISP1 канал и в случае обнаружения его отказа трафик будет направлен по резервному ISP2 каналу. После восстановления работы основного ISP1 провайдера, прохождение полезного трафика будет возвращено на основной VPN-туннель. Переключение между туннелями осуществляется с помощью периодически запускаемого скрипта (каждые 15 секунд), созданного на обоих VPN-шлюзах. Скрипт проверяет доступность виртуального tap-интерфейса основного соединения соседнего VPN-шлюза и, в случае его недоступности, заменяет маршрут к удаленной подсети через резервное соединение. После восстановления работы основного провайдера произойдет автоматическая замена маршрута для работы через основное подключение.

3. Описание устройства «Router1»

Устройство «Router1» – маршрутизатор, обеспечивающий следующие функции:

- Доступ центрального офиса в неконтролируемый сегмент (Интернет) через два провайдера;
- Маршрутизацию трафика между центральной и удаленной площадкой. Для этого добавлен статический маршрут вида: 192.168.2.0/24 via 10.1.1.2;
- Проброс TCP-порта 1355 (DNAT) с внешних интерфейсов маршрутизатора Ge0/0:172.21.21.2 и Ge0/1:172.22.22.2 на сетевой интерфейс ens3:10.2.2.2 VPN-сервера «SCR1».

4. Описание устройства «Router2»

Устройство «Router2» – маршрутизатор, обеспечивающий следующие функции:

- Доступ центрального офиса в неконтролируемый сегмент (Интернет) через два провайдера;
- Маршрутизацию трафика между удаленной и центральной площадкой. Для этого добавлен статический маршрут вида: 192.168.1.0/24 via 10.2.2.2

5. Описание устройства «Host1»

Устройство «Host1» – рабочее место администратора с операционной системой Windows 7 на сетевом интерфейсе которого назначен статический ip-адрес 192.168.1.2/24 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.

6. Описание устройства «Host2»

Устройство «Host2» – рабочее место администратора с операционной системой Windows 7 на сетевом интерфейсе которого назначен статический ip-адрес 192.168.2.2/24 gw 192.168.2.1 и установлен программный продукт «S-Crypto VPN Server Manager» для удаленного администрирования VPN-сервера «SCR2» с помощью графического пользовательского интерфейса.

7. Описание устройства «SCR1»

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

7.1 Настройка операционной системы

- Разрешено прохождение трафика между интерфейсами. В файле /etc/sysctl.conf добавлен параметр

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

- Назначены адреса на интерфейсах. Содержимое файла /etc/network/interfaces

```
auto lo
iface lo inet loopback
```

```
allow-hotplug ens3
iface ens3 inet static
address 10.1.1.2/24
gateway 10.1.1.1
```

```
allow-hotplug tap_1
iface tap_1 inet static
address 10.0.5.1/24
```

```
allow-hotplug tap_2
iface tap_2 inet static
address 10.0.6.1/24
```

7.2 Создание скрипта и настройка его запуска

- Создать файл скрипта для замены маршрута, например командой nano /opt/replace-routes.sh, со следующим содержанием:

```
#!/bin/bash
```

```
R_SUBNET="192.168.2.0/24" #удаленная подсеть
MAIN_GATEWAY="10.0.5.2" #основной tap на соседнем шлюзе
BACKUP_GATEWAY="10.0.6.2" #резервный tap на соседнем шлюзе
```

```
if ping -c 4 "$MAIN_GATEWAY " | grep -q "ttl="; then
    ip route replace "$R_SUBNET " via "$MAIN_GATEWAY"
else
    ip route replace "$R_SUBNET " via "$BACKUP_GATEWAY"
fi
```

- Сделать файл исполняемым следующей командой:

```
chmod +x /opt/replace-routes.sh
```

- Создать сервис для выполнения созданного скрипта командой `nano /etc/systemd/system/replace-routes.service` со следующим содержанием:

```
[Unit]
Description=Replace routes
After=network.target

[Service]
Type=simple
ExecStart=/opt/replace_routes.sh
Restart=always

[Install]
WantedBy=multi-user.target
```

- Создать таймер для периодического (каждые 15 секунд) запуска созданного сервиса командой `nano /etc/systemd/system/replace-routes.timer` со следующим содержанием:

```
[Unit]
Description=Timer for replace_routes

[Timer]
OnBootSec=30s
OnUnitActiveSec=15s
Unit=replace_routes.service

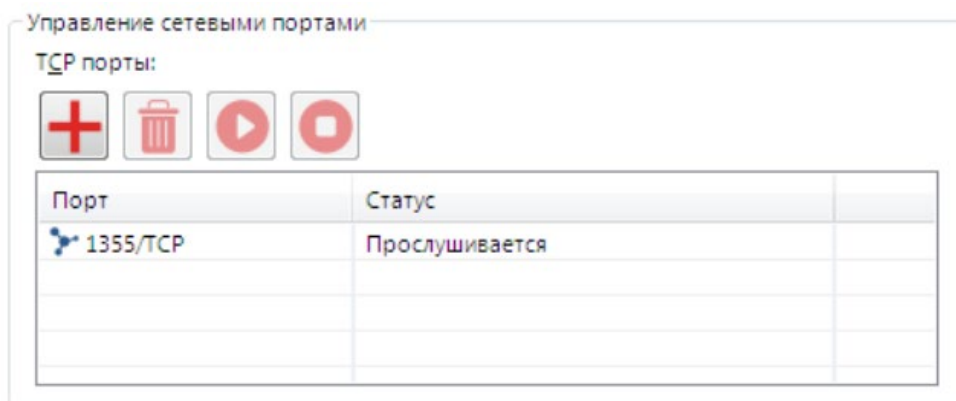
[Install]
WantedBy=timers.target
```

- Примените изменения и запустите таймер командами:

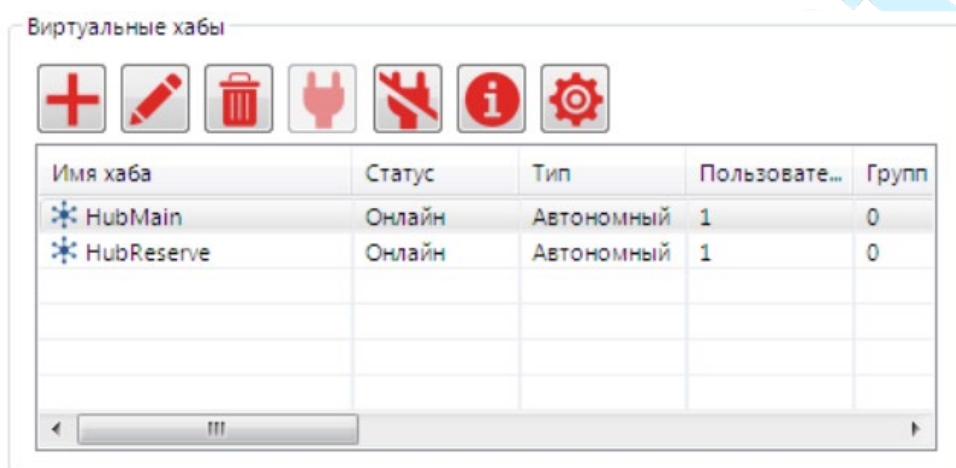
```
sudo systemctl daemon-reload
sudo systemctl enable replace_routes.timer
sudo systemctl start replace_routes.timer
```

7.3 Настройка «S-Crypto VPN Server»

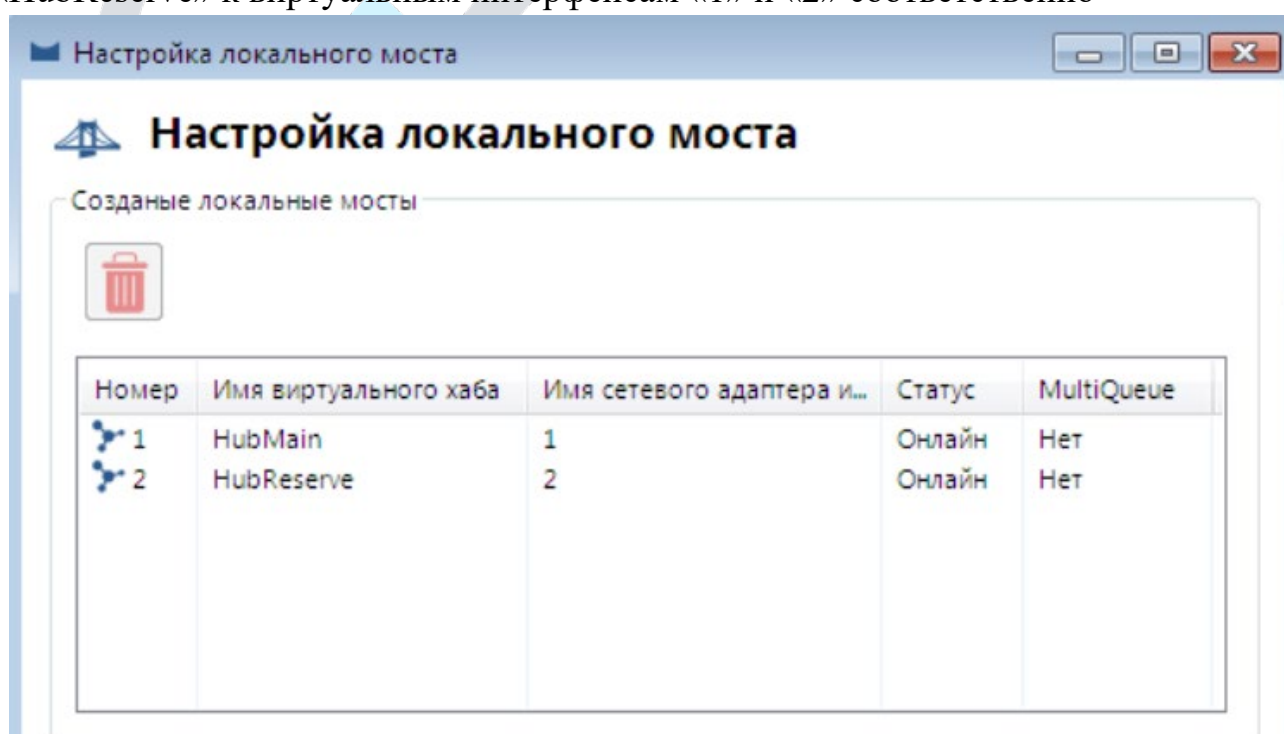
- Для обработки входящих подключений включен для прослушивания порты TCP:1355



- На сервере созданы виртуальные хабы с именами «HubMain» и «HubReserve»



- Созданы локальные мосты от виртуальных хабов «HubMain» и «HubReserve» к виртуальным интерфейсам «1» и «2» соответственно



- На виртуальных хабах созданы пользователи, от имени которых производится аутентификация входящих подключений.

Список пользователей виртуального хаба «HubMain»

Имя пользователя	Полное имя	Имя группы	Описание	Метод аутентификации
UserMG		-		Парольная аутентификация

Список пользователей виртуального хаба «HubReserve»

Имя пользователя	Полное имя	Имя группы	Описание	Метод аутентификации
UserRG		-		Парольная аутентификация

8. Описание устройства «SCR2»

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

8.1 Настройка операционной системы

- Разрешено прохождение трафика между интерфейсами. В файле `/etc/sysctl.conf` добавлен параметр `net.ipv4.ip_forward = 1`

- Назначены адреса на интерфейсах. Содержимое файла `/etc/network/interfaces`

```
auto lo
iface lo inet loopback
```

```
allow-hotplug ens3
iface ens3 inet static
address 10.2.2.2/24
gateway 10.2.2.1
```

```
allow-hotplug tap_1
iface tap_1 inet static
address 10.0.5.2/24
```

```
allow-hotplug tap_2
iface tap_2 inet static
address 10.0.6.2/24
```

8.2 Создание скрипта и настройка его запуска

- Создать файл скрипта для замены маршрута, например командой `nano /opt/replace-routes.sh`, со следующим содержанием:

```
#!/bin/bash

R_SUBNET="192.168.1.0/24" #удаленная подсеть
MAIN_GATEWAY="10.0.5.1" #основной tap на соседнем шлюзе
BACKUP_GATEWAY="10.0.6.1" #резервный tap на соседнем шлюзе

if ping -c 4 "$MAIN_GATEWAY " | grep -q "ttl="; then
    ip route replace "$R_SUBNET " via "$MAIN_GATEWAY"
else
    ip route replace "$R_SUBNET " via "$BACKUP_GATEWAY"
fi
```

- Сделать файл исполняемым следующей командой:
`chmod +x /opt/replace-routes.sh`

- Создать сервис для выполнения созданного скрипта командой `nano /etc/systemd/system/replace-routes.service` со следующим содержанием:

```
[Unit]
Description=Replace routes
After=network.target

[Service]
Type=simple
ExecStart=/opt/replace_routes.sh
Restart=always

[Install]
WantedBy=multi-user.target
```

- Создать таймер для периодического (каждые 15 секунд) запуска созданного сервиса командой `nano /etc/systemd/system/replace-routes.timer` со следующим содержанием:

```
[Unit]
Description=Timer for replace_routes
```

```
[Timer]
OnBootSec=30s
OnUnitActiveSec=15s
Unit=replace_routes.service
```

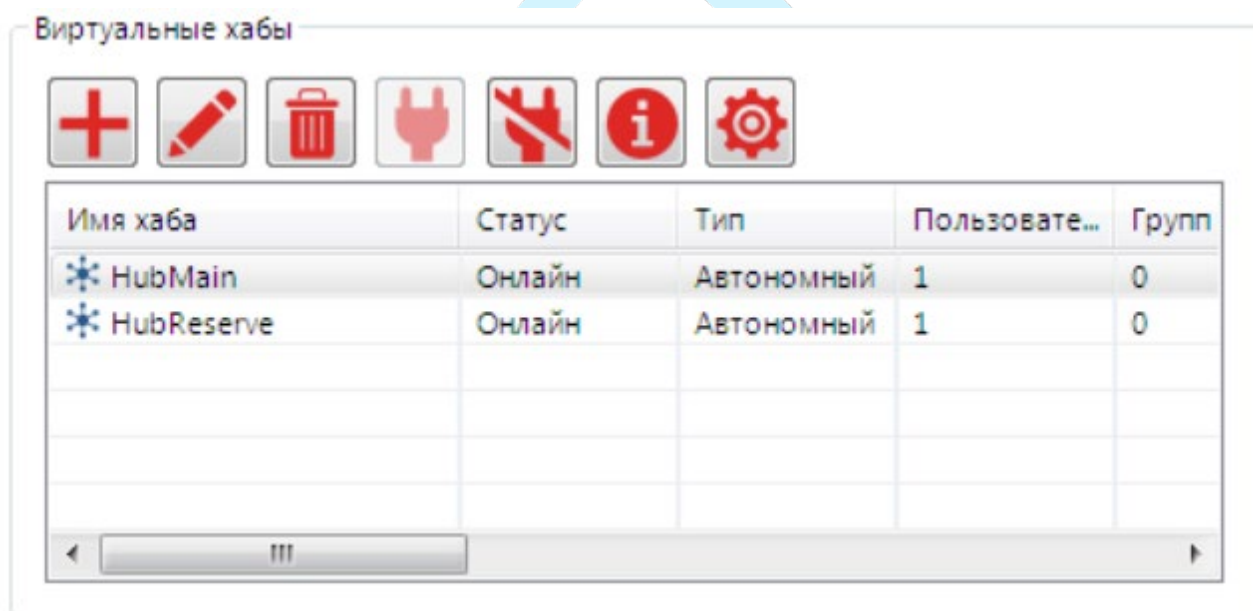
```
[Install]
WantedBy=timers.target
```

- Примените изменения и запустите таймер командами:

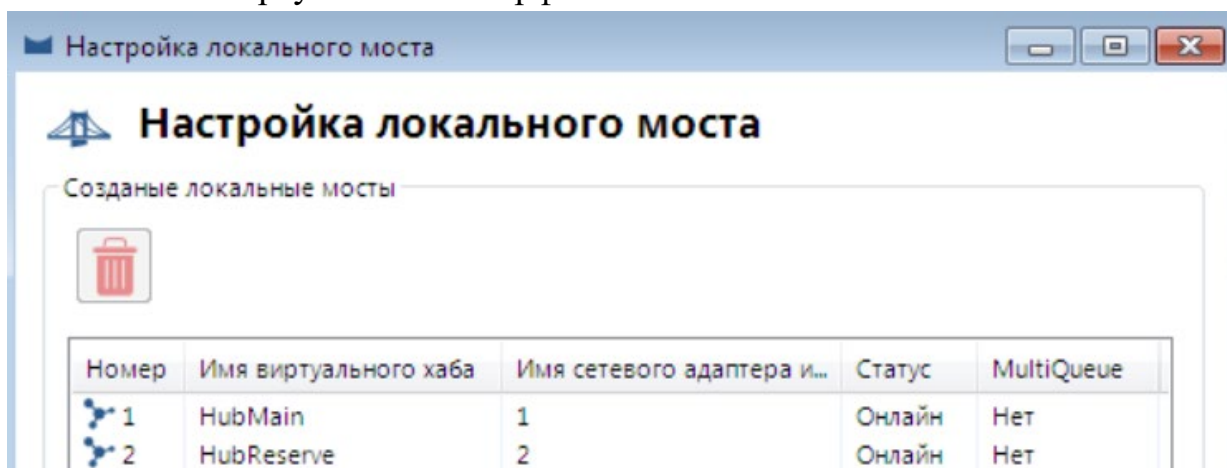
```
sudo systemctl daemon-reload
sudo systemctl enable replace_routes.timer
sudo systemctl start replace_routes.timer
```

8.3 Настройка «S-Crypto VPN Server»

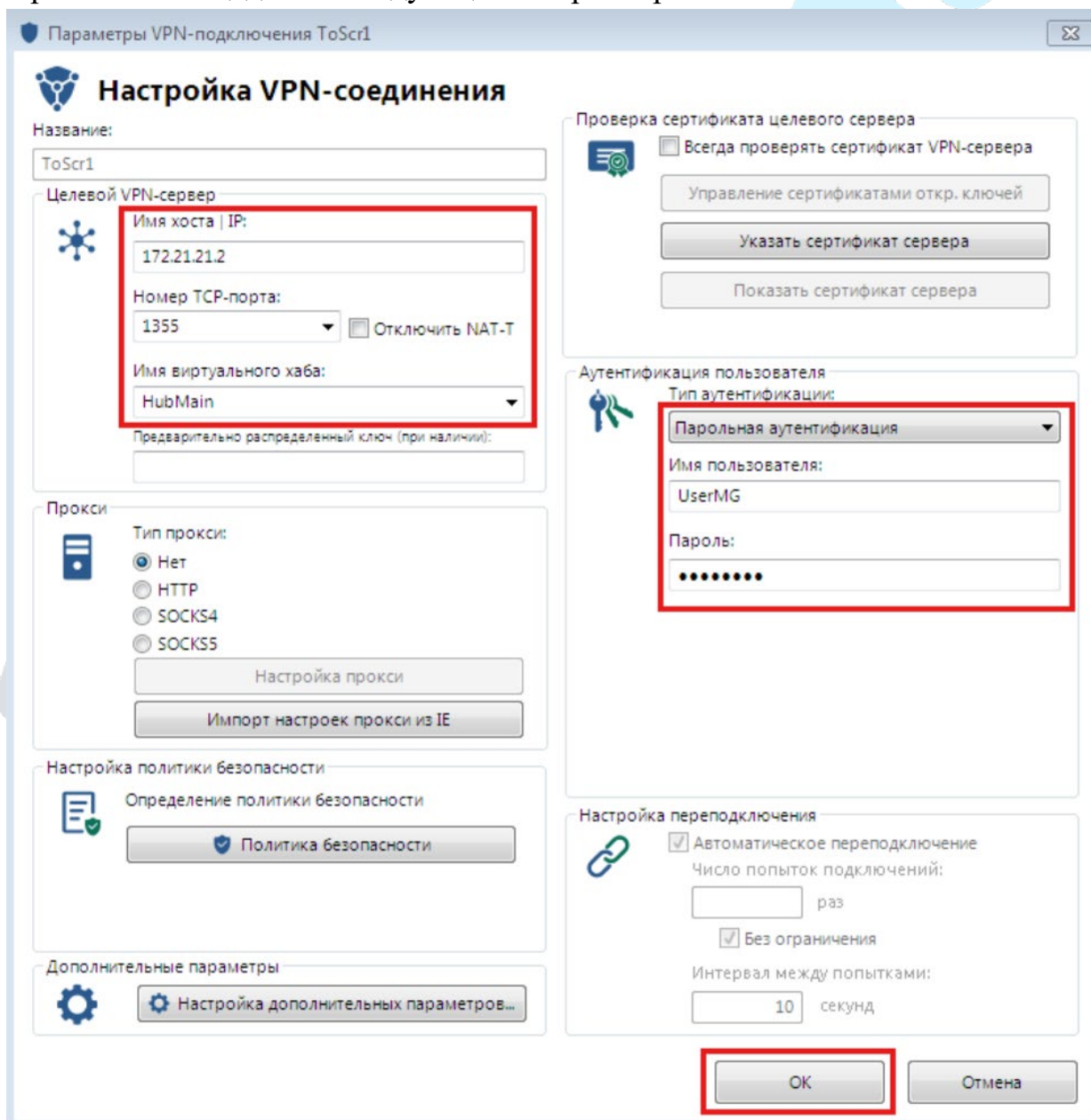
- На сервере созданы виртуальные хабы с именами «HubMain» и «HubReserve»



- Созданы локальные мосты от виртуальных хабов «HubMain» и «HubReserve» к виртуальным интерфейсам «1» и «2» соответственно



- В настройках виртуального хаба «HubMain» в разделе «Соединения с удаленными сетями» создано одно подключение через основного провайдера центральной площадки со следующими параметрами



- В настройках виртуального хаба «HubReserve» в разделе «Соединения с удаленными сетями» создано одно подключение через резервного провайдера центральной площадки со следующими параметрами

Параметры VPN-подключения ToScr1R

Настройка VPN-соединения

Название: ToScr1R

Целевой VPN-сервер

Имя хоста | IP: 172.22.22.2

Номер TCP-порта: 1355 Отключить NAT-T

Имя виртуального хаба: HubReserve

Предварительно распределенный ключ (при наличии):

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: UserRG

Пароль:

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...

Настройка переподключения

Автоматическое переподключение

Число попыток подключений: раз

Без ограничения

Интервал между попытками: 10 секунд

OK Отмена