

S-CRYPTO VPN 1.0

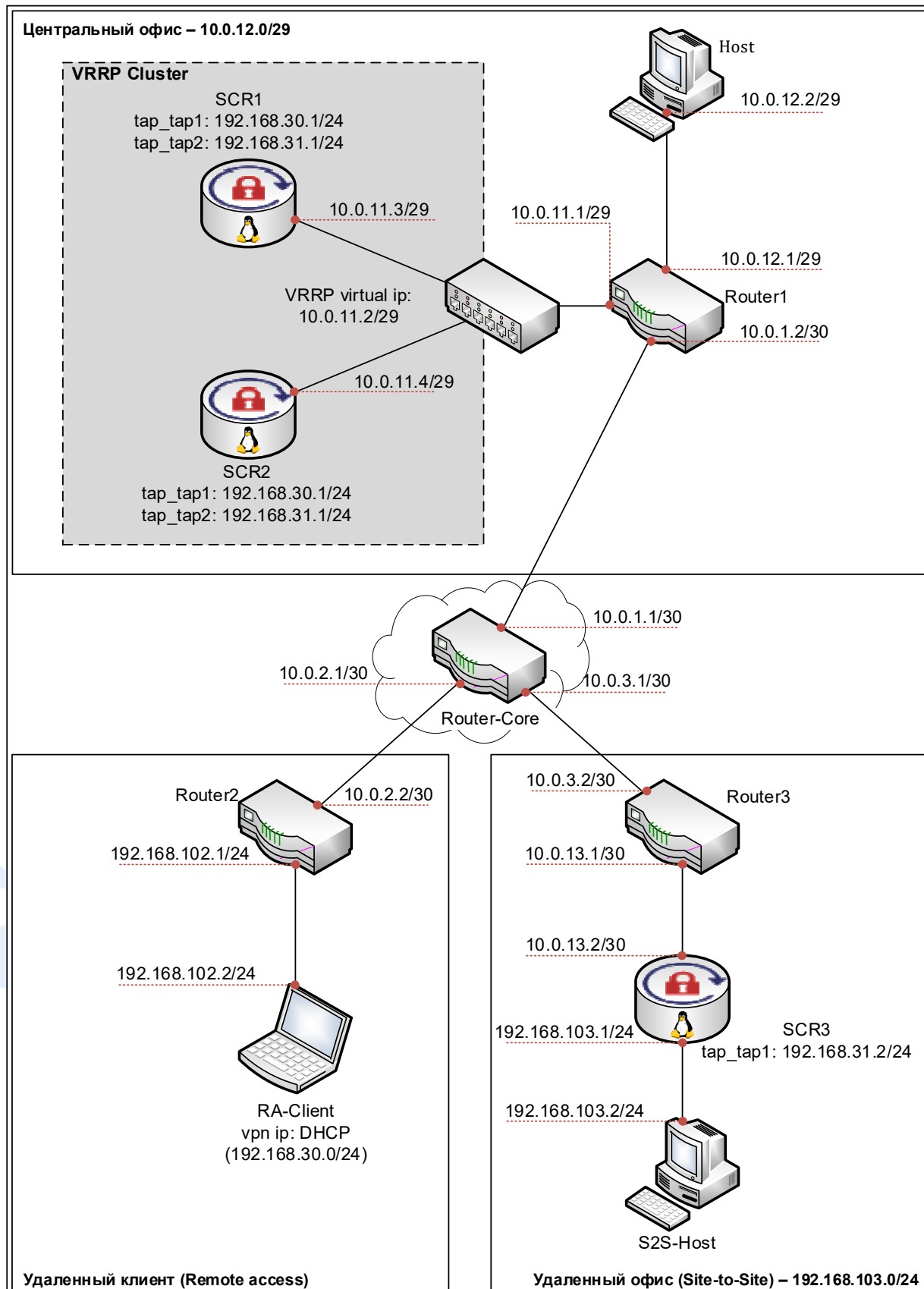
Построение отказоустойчивого решения на базе протокола VRRP с подключением шлюзов «S-Crypto VPN Server» методом Router-on-Stick

Оглавление

1. Описание стенда.....	2
2. Логика работы кластера.....	3
3. Описание устройства «Router-Core».....	4
4. Описание устройства «Router1»	4
5. Описание устройства «Router2»	5
6. Описание устройства «Router3»	5
7. Описание устройства «Host»	6
8. Описание устройства «S2S-Host».....	6
9. Описание устройства «RA-Client».....	6
10. Описание устройства «SCR1».....	7
10.1 Настройка операционной системы	7
10.2 Настройка «S-Crypto VPN Server»	8
11. Описание устройства «SCR2».....	10
11.1 Настройка операционной системы	10
11.2 Настройка «S-Crypto VPN Server»	11
12. Описание устройства «SCR3».....	12
12.1 Настройка операционной системы	12
12.2 Настройка «S-Crypto VPN Server»	12
Приложение 1. Альтернативная конфигурация кластера.....	15

1. Описание стенда

Сценарий содержит пример построения защищенного соединения между двумя подсетями (Site-to-Site), а также подключение удаленных клиентов (Remote Access). Центральная площадка 10.0.12.0/29, защищается парой шлюзов безопасности «S-Crypto VPN Server» SCR1 и SCR2, подключенных методом Router-on-Stick, объединенных в отказоустойчивый кластер. Пары устройств «Host» – «S2S-Host» и «Host» – «RA-Client» связаны защищенными VPN соединениями. Отказоустойчивость кластера реализована с помощью протокола VRRP.



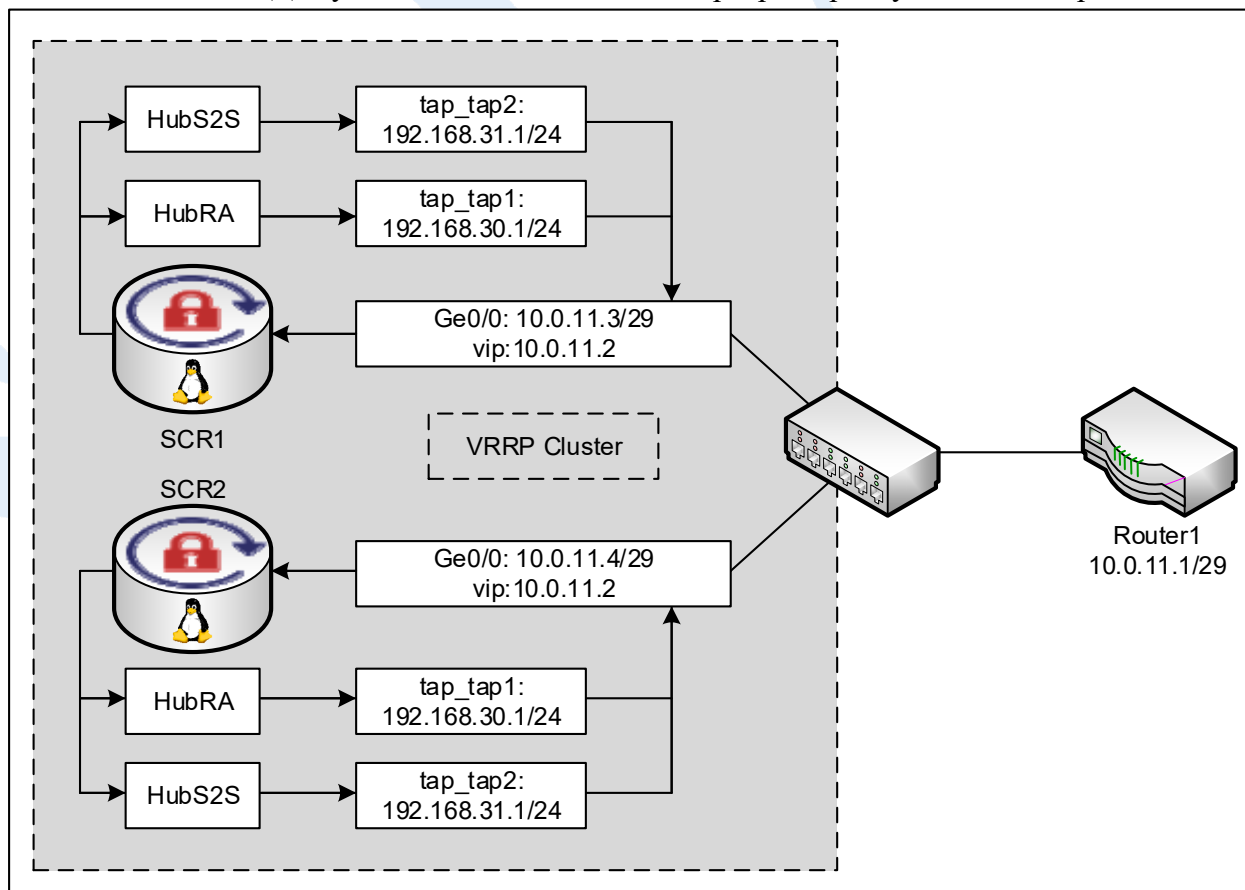
2. Логика работы кластера

Шлюзы «SCR1» и «SCR2» объединены в отказоустойчивый кластер, работающий на базе протокола VRRP с использованием пакета «keepalived». При использовании протокола VRRP ноды кластера имеют виртуальный адрес (VIP). Один из шлюзов является главным (Master), а второй резервным (Backup). Нода, находящаяся в состоянии Master, владеет VIP адресом и, соответственно, обрабатывает трафик. В случае отработки отказа (типы отказов описаны далее) основная нода становится недоступной и её статус меняется с Master на Fault, при этом состояние резервной ноды переходит с Backup на Master и продолжает обрабатывать трафик. При возвращении в строй основной ноды для уменьшения количества переключений перехват VIP-адреса не происходит. Обнаружение недоступности ноды, находящейся в состоянии Master, происходит благодаря рассылке основной (Master) нодой служебных пакетов протокола VRRP (advertisement messages) в которых адрес источника – основной IP-адрес интерфейса, на котором включен VRRP, а IP-адрес назначения – 224.0.0.18. Если резервная нода в состоянии Backup перестает получать от основной ноды на всех синхронизированных интерфейсах пакеты VRRP Advertisement messages, то она захватывает роль Master.

Кластер VRRP обрабатывает следующие типы отказов:

- отключение питания;
- выход из строя аппаратной платформы;
- отказ сетевого интерфейса;
- отказ порта на коммутационном оборудовании;
- отключение виртуальных интерфейсов;
- отключение виртуальных хабов на VPN сервере;
- отключение службы VPN сервера.

Для обеспечения одновременного обслуживания разных типов подключений, на каждом VPN-сервере будут созданы по два виртуальных хаба. «HubS2S» для «Site-to-Site» и «HubRA» для «Remote Access». Для установки соединения на серверах прослушивается порт TCP:1355.



3. Описание устройства «Router-Core»

Устройство «Router-Core» – маршрутизатор на базе Debian в котором настроены следующие параметры:

- 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 10.0.1.1
netmask 255.255.255.252
```

```
allow-hotplug ens4 iface
ens4 inet static
address 10.0.2.1
netmask 255.255.255.252
```

```
allow-hotplug ens5
iface ens5 inet static
address 10.0.3.1
netmask 255.255.255.252
```

4. Описание устройства «Router1»

Устройство «Router1» – маршрутизатор на базе Debian в котором настроены следующие параметры:

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

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

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

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

```
allow-hotplug ens3
iface ens3 inet static
address 10.0.1.2
netmask 255.255.255.252
gateway 10.0.1.1
```

```
allow-hotplug ens4 iface
ens4 inet static
address 10.0.11.1
netmask 255.255.255.248
post-up ip route add 192.168.30.0/24 via 10.0.11.2
post-up ip route add 192.168.31.0/24 via 10.0.11.2
post-up ip route add 192.168.103.0/24 via 10.0.11.2
pre-down ip route del 192.168.30.0/24 via 10.0.11.2
pre-down ip route del 192.168.31.0/24 via 10.0.11.2
pre-down ip route del 192.168.103.0/24 via 10.0.11.2
```

```
allow-hotplug ens5
```

```
iface ens5 inet static
address 10.0.12.1
netmask 255.255.255.248
```

- Настроены правила трансляции адресов в iptables

```
iptables -t nat -A PREROUTING -p tcp --dport 1355 -j DNAT --to-destination 10.0.11.2
iptables -t nat -A POSTROUTING -o ens3 -j MASQUERADE
```

5. Описание устройства «Router2»

Устройство «Router2» – маршрутизатор на базе Debian в котором настроены следующие параметры:

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

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

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

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

```
allow-hotplug ens3
iface ens3 inet static
address 10.0.2.2
netmask 255.255.255.252
gateway 10.0.2.1
```

```
allow-hotplug ens4 iface
ens4 inet static
address 192.168.102.1
netmask 255.255.255.0
```

- Настроены правила трансляции адресов в iptables

```
iptables -t nat -A POSTROUTING -o ens3 -j MASQUERADE
```

6. Описание устройства «Router3»

Устройство «Router3» – маршрутизатор на базе Debian в котором настроены следующие параметры:

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

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

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

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

```
allow-hotplug ens3
iface ens3 inet static
address 10.0.3.2
netmask 255.255.255.252
gateway 10.0.3.1
```

```
allow-hotplug ens4 iface
ens4 inet static
address 10.0.13.1
netmask 255.255.255.252
post-up ip route add 192.168.103.0/24 via 10.0.13.2
```

```
pre-down ip route del 192.168.103.0/24 via 10.0.13.2
```

- Настроены правила трансляции адресов в iptables

```
iptables -t nat -A POSTROUTING -o ens3 -j MASQUERADE
```

7. Описание устройства «Host»

Устройство «Host» – сетевое устройство с назначенным на сетевом интерфейсе статическим ip-адресом 10.0.12.2/29 gw 10.0.12.1. Используется в сценарии для тестирования доступности устройств в локальной сети центрального офиса.

8. Описание устройства «S2S-Host»

Устройство «S2S-Host» – сетевое устройство с назначенным на сетевом интерфейсе статическим ip-адресом 192.168.103.2/24 gw 192.168.103.1. Используется в сценарии для тестирования доступности устройств в локальной сети удаленного офиса.

9. Описание устройства «RA-Client»

Устройство «RA-Client» – удаленное рабочее место на базе операционной системы Windows 7 x86 на физическом сетевом интерфейсе которого назначен статический ip-адрес 192.168.102.2/24 gw 192.168.102.1. Для установления защищенного соединения к центральной площадке на устройстве установлен продукт «S-Crypto VPN Client» в котором создано VPN-соединение со следующими параметрами:

The screenshot shows the 'Настройка VPN-соединения' (VPN Connection Settings) window for a connection named 'to VRRP'. The window is divided into several sections:

- Целевой VPN-сервер (Target VPN Server):** Hostname/IP is '10.0.12', TCP port is '1355'. There is a checkbox for 'Отключить NAT-T' (Disable NAT-T) which is currently unchecked. The virtual hub name is 'HubRA'.
- Прокси (Proxy):** Type is set to 'Нет' (None). Buttons for 'Настройка прокси' and 'Импорт настроек прокси из IE' are present.
- Виртуальный сетевой адаптер (Virtual Network Adapter):** A dropdown menu shows 'VPN Client Adapter - VPN'.
- Дополнительные параметры (Additional Parameters):** Includes a button for 'Настройка дополнительных параметров...'. At the bottom, there are checkboxes for 'Скрыть экраны состояния и ошибок' and 'Скрыть экраны IP-адресов'.
- Проверка сертификата целевого сервера (Target Server Certificate Check):** Includes a checkbox for 'Всегда проверять сертификат VPN-сервера' (Always check VPN server certificate) which is unchecked. Buttons for 'Управление сертификатами откр. ключей', 'Указать сертификат сервера', and 'Показать сертификат сервера' are available.
- Аутентификация пользователя (User Authentication):** Type is 'Парольная аутентификация' (Password authentication). Username is 'UserRA'. The password field is masked with dots. A button 'Изменить пароль' (Change password) is present.
- Настройка переподключения (Reconnection Settings):** Includes a checked checkbox for 'Автоматическое переподключение' (Automatic reconnection). The number of attempts is set to '1 раз' (1 time). There is a checked checkbox for 'Без ограничения' (Without limit). The interval between attempts is set to '5 секунд' (5 seconds).

At the bottom right, there are 'OK' and 'Отмена' (Cancel) buttons.

10. Описание устройства «SCR1»

Шлюз безопасности «SCR1» – устройство на базе операционной системы Debian с установленным пакетом «keepalived», для работы VRRP-кластера, и установленным продуктом «S-Crypto VPN Server».

10.1 Настройка операционной системы

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

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

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

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

```
allow-hotplug ens3
iface ens3 inet static
address 10.0.11.3
netmask 255.255.255.248
gateway 10.0.11.1
```

```
allow-hotplug tap_tap1
iface tap_tap1 inet static
address 192.168.30.1
netmask 255.255.255.0
```

```
allow-hotplug tap_tap2
iface tap_tap2 inet static
address 192.168.31.1
netmask 255.255.255.0
post-up ip route add 10.0.103.0/24 via 192.168.31.2
pre-down ip route del 10.0.103.0/24 via 192.168.31.2
```

- Создан файл конфигурации `/etc/keepalived/keepalived.conf` со следующими параметрами работы VRRP

```
global_defs {
    dynamic-interfaces
    vrrp_garp_master_refresh 30
    vrrp_garp_master_refresh_repeat 2
}
vrrp_sync_group group1 {
    group {
        ens3_0
    }
}
vrrp_track_process scrypto {
    process vpnserver
    quorum 1
    delay 5
}
vrrp_instance ens3_0 {
    state BACKUP
    version 3
    interface ens3
    virtual_router_id 23
    priority 110
    advert_int 3
```



```

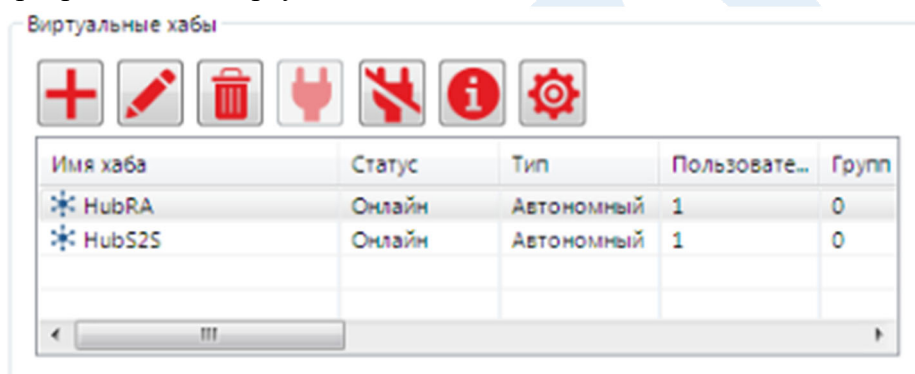
nopreempt
virtual-ipaddress {
    10.0.11.2
}
track_interface {
    ens3
    tap_tap1
    tap_tap2
}
track_process {
    scrypto
}
}

```

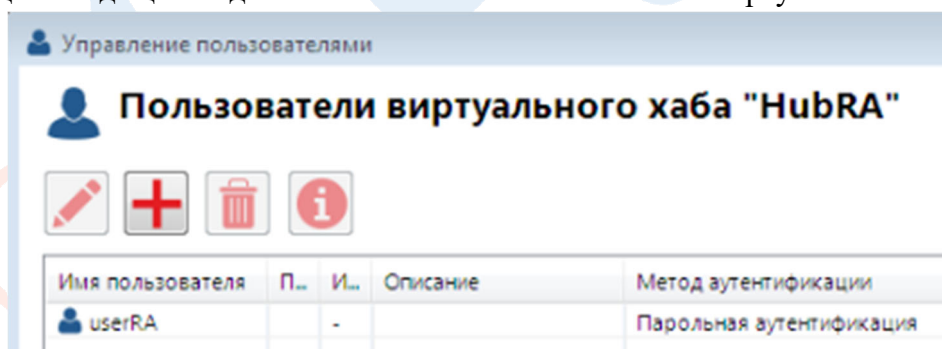
- Сервис keepalived запущен и добавлен в автозапуск командами
`sudo systemctl start keepalived`
`sudo systemctl enable keepalived`

10.2 Настройка «S-Crypto VPN Server»

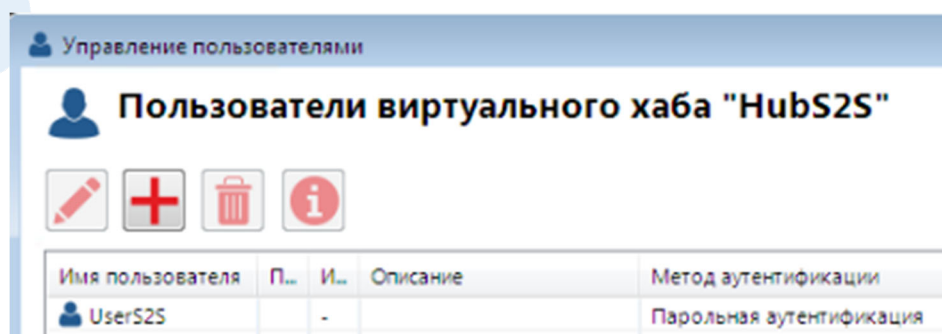
- На сервере созданы виртуальные хабы с именами «HubRA» и «HubS2S»



- На виртуальных хабах созданы пользователи, от имени которых производится аутентификация входящих подключений. Список пользователей виртуального хаба «HubRA»



Список пользователей виртуального хаба «HubS2S»



- На виртуальном хабе «HubRA» запущен DHCP-сервер со следующими параметрами

Конфигурация виртуального NAT и DHCP

Конфигурация виртуального NAT и DHCP на хабе "HubRA"

Настройки сетевого интерфейса виртуального хоста

MAC-адрес: 5E-22-2F-82-03-F3

IP-адрес: 192.168.30.254

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

☒ Сохранить операции NAT и DHCP-сервера в журнале событий

OK Отмена

Редактирование таблицы статической маршрутизации

Таблица статической маршрутизации для VPN-клиентов

10.0.12.0/255.255.255.0/192.168.30.1

Примечание: Каждая запись должна быть указана в формате "IP-адрес сети/маска подсети/IP-адрес шлюза". Для разделения нескольких записей (максимум: 64 записей) можно использовать запятые или пробелы. Пример: 192.168.23.0/255.255.255.0/192.168.0.1, 10.0.0.0/255.0.0.0/192.168.0.2

Виртуальный DHCP-сервер поддерживает использование бесклассовых статических маршрутов (RFC 3442). Если используется внешний DHCP-сервер, то необходимо выключить виртуальный DHCP-сервер.

Для реализации раздельного туннелирования в параметрах виртуального DHCP-сервера необходимо очистить поле шлюза по умолчанию.

OK Отмена

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

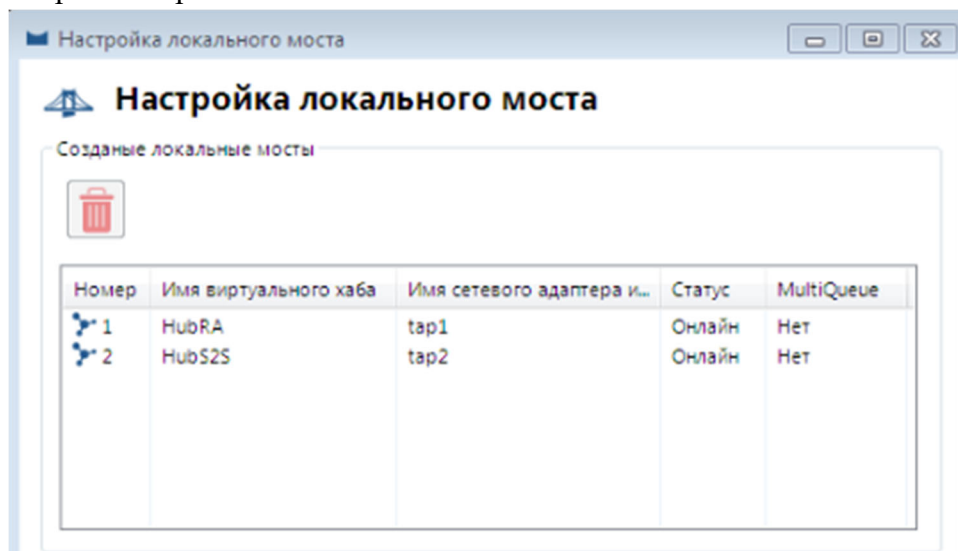
Управление сетевыми портами

TCP порты:

+ - > <

Порт	Статус
1355/TCP	Прослушивается

- Созданы локальные мосты от виртуальных хабов «HubRA» и «HubS2S» к виртуальным интерфейсам «tap1» и «tap2» соответственно



11. Описание устройства «SCR2»

Шлюз безопасности «SCR2» – устройство на базе операционной системы Debian с установленным пакетом «keepalived», для работы VRRP-кластера, и установленным продуктом «S-Crypto VPN Server».

11.1 Настройка операционной системы

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

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

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

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

```
allow-hotplug ens3
iface ens3 inet static
address 10.0.11.4
netmask 255.255.255.248
gateway 10.0.11.1
```

```
allow-hotplug tap_tap1
iface tap_tap1 inet static
address 192.168.30.1
netmask 255.255.255.0
```

```
allow-hotplug tap_tap2
iface tap_tap2 inet static
address 192.168.31.1
netmask 255.255.255.0
post-up ip route add 10.0.103.0/24 via 192.168.31.2
pre-down ip route del 10.0.103.0/24 via 192.168.31.2
```

- Создан файл конфигурации /etc/keepalived/keepalived.conf со следующими параметрами работы VRRP

```
global_defs {
    dynamic-interfaces
    vrrp_garp_master_refresh 30
```

```

    vrrp_garp_master_refresh_repeat 2
}
vrrp_sync_group group1 {
    group {
        ens3_0
    }
}
vrrp_track_process scrypto {
    process vpnsver
    quorum 1
    delay 5
}
vrrp_instance ens3_0 {
    state BACKUP
    version 3
    interface ens3
    virtual_router_id 23
    priority 90
    advert_int 3
    nopreempt
    virtual-ipaddress {
        10.0.11.2
    }
    track_interface {
        ens3
        tap_tap1
        tap_tap2
    }
    track_process {
        scrypto
    }
}

```

- Сервис keepalived запущен и добавлен в автозапуск командами

```

sudo systemctl start keepalived
sudo systemctl enable keepalived

```

11.2 Настройка «S-Crypto VPN Server»

- Параметры сервера «S-Crypto VPN Server» на ноде «SCR2» идентичны параметрам на ноде «SCR1» которые представлены в пункте 10.2 этого сценария.

12. Описание устройства «SCR3»

Шлюз безопасности «SCR3» – устройство на базе операционной системы Debian с установленным продуктом «S-Crypto VPN Server».

12.1 Настройка операционной системы

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

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

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

```
auto lo
```

```
iface lo inet loopback
```

```
allow-hotplug ens3
```

```
iface ens3 inet static
```

```
address 10.0.13.2
```

```
netmask 255.255.255.252
```

```
gateway 10.0.13.1
```

```
allow-hotplug ens4
```

```
iface ens4 inet static
```

```
address 192.168.103.1
```

```
netmask 255.255.255.0
```

```
allow-hotplug tap_tap1
```

```
iface tap_tap1 inet static
```

```
address 192.168.31.2
```

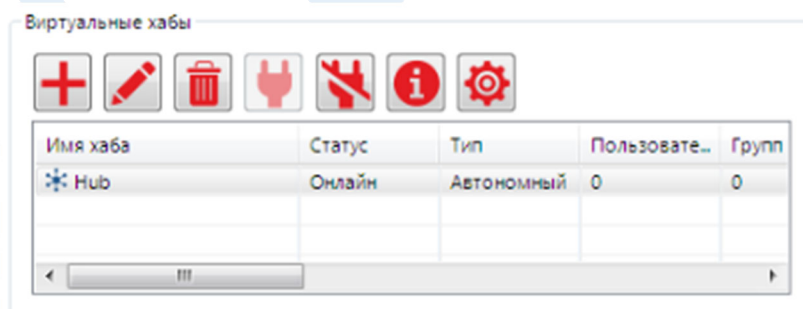
```
netmask 255.255.255.0
```

```
post-up ip route add 10.0.12.0/24 via 192.168.31.1
```

```
pre-down ip route del 10.0.12.0/24 via 192.168.31.1
```

12.2 Настройка «S-Crypto VPN Server»

- На сервере создан виртуальный хаб с именем «Hub»



- В настройках виртуального хаба «Hub» в разделе «Соединения с удаленными сетями» создано одно подключение к кластеру центральной площадки со следующими параметрами

Параметры VPN-подключения to VRRP

Настройка VPN-соединения

Название: to VRRP

Целевой VPN-сервер

Имя хоста | IP: 10.0.1.2

Номер TCP-порта: 1355 ☐ Отключить NAT-T

Имя виртуального хаба: HubS2S

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: userS2S

Пароль:

Настройка переключения

☒ Автоматическое переключение

Число попыток подключений: раз

☒ Без ограничения

Интервал между попытками: 10 секунд

OK Отмена

- Создан локальный мост от виртуального хаба «Hub» к виртуальному интерфейсу «tap1»

Настройка локального моста

Настройка локального моста

Созданные локальные мосты

Номер	Имя виртуального хаба	Имя сетевого адаптера и...	Статус	MultiQueue
1	Hub	tap1	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:

tap1

(< 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

Приложение 1. Альтернативная конфигурация кластера

Если предполагается, что нода «SCR1» в кластере всегда имеет статус «Master» и при восстановлении её работы после сбоя обработка трафика и VIP-адрес всегда возвращается основной ноде «SCR1», а статус ноды «SCR2» принимает значение «Backup», то необходимо изменить конфигурацию VRRP следующим образом:

- Нода «SCR1». Параметры в файле конфигурации /etc/keepalived/keepalived.conf

```
global_defs {
    dynamic-interfaces
    vrrp_garp_master_refresh 30
    vrrp_garp_master_refresh_repeat 2
}
vrrp_sync_group group1 {
    group {
        ens3_0
    }
}
vrrp_track_process scrypto {
    process vpnserv
    quorum 1
    delay 5
}
vrrp_instance ens3_0 {
    state MASTER
    version 3
    interface ens3
    virtual_router_id 23
    priority 110
    advert_int 3
    virtual-ipaddress {
        10.0.11.2
    }
    track_interface {
        ens3
        tap_tap1
        tap_tap2
    }
    track_process {
        scrypto
    }
}
```

- Нода «SCR2». Параметры в файле конфигурации /etc/keepalived/keepalived.conf

```
global_defs {
    dynamic-interfaces
    vrrp_garp_master_refresh 30
    vrrp_garp_master_refresh_repeat 2
}
vrrp_sync_group group1 {
    group {
        ens3_0
    }
}
vrrp_track_process scrypto {
    process vpnserv
    quorum 1
    delay 5
}
```



```
}  
vrrp_instance ens3_0 {  
    state BACKUP  
    version 3  
    interface ens3  
    virtual_router_id 23  
    priority 90  
    advert_int 3  
    virtual-ipaddress {  
        10.0.11.2  
    }  
    track_interface {  
        ens3  
        tap_tap1  
        tap_tap2  
    }  
    track_process {  
        scrypto  
    }  
}
```