Использование модемов в «С-Терра Шлюз» 5.0

Назначение документа

Документ описывает ряд необходимых процедур, которые нужно выполнить на «С-Терра Шлюз», чтобы реализовать возможность по использованию модема в качестве канала связи.

Список поддерживаемых модемов

Производителем проверена поддержка следующих USB-модемов с «С-Терра Шлюз» 5.0:

- Alcatel IK41VE1-2AALRU1;
- Alcatel IK41VE1-2BALRU1;
- DEXP M1;
- DEXP M2;
- Digma Dongle DW1960;
- Huawei E3372h-607;
- Huawei Brovi E3372-325 – требуется обновление прошивки. Подробности смотрите в Приложении;
- Huawei E3372h-153;
- Huawei E8372h-320;
- LTE 4G WIFI Dongle;
- OLAX U90-E;
- Tenda 4G01;
- ZTE F30 Pro;
- ZTE MF79N;
- ZTE MF79RU;
- ZTE MF833N;
- ZTE MF833T.

Производителем проверена поддержка следующих Mini PCI модемов с «С-Терра Шлюз» 5.0:

- SIMCom SIM7600E-H – QMI-модем.
- Quectel EP06-E – QMI-модем. Поддерживается, однако в текущей версии пакета `stmodems` в файле журнала может выводиться сообщение о том, что это не поддерживаемая модель модема. Этот вывод исправлен в версиях `stmodems` новее `0.3+sterra1-debian12`.

  Для каждого QMI-модема требуется проверить данные о ПО. Подробности смотрите в Приложении.

Если модема нет в списке поддерживаемых модемов и он отсутствует в списке неподдерживаемых модемов, то совместимость модема с «С-Терра Шлюз» может быть проверена самостоятельно в соответствии с критериями, изложенными в Приложении.

Список неподдерживаемых модемов

Следующие USB-модемы не будут работать с «С-Терра Шлюз» 5.0:

- Anydata W140;
- Digma Dongle DW1961;
- DQ431.

Ограничения и особенности

1. Модем должен быть совместим с «С Терра Шлюз» 5.0 в соответствии с требованиями, изложенными в главе «Список поддерживаемых модемов».
2. Обратите внимание на то, что встречаются случаи, когда на штатной прошивке внутренние подсети модемов невозможно изменить, например у модема Huawei E3372h-153 – это подсеть 192.168.8.0/24.

3. Если на модеме отсутствуют функции DMZ или Port Forwarding, то «С-Терра Шлюз» не может выступать в роли ответчика защищенных/незащищенных соединений. То есть, если на модеме нельзя настроить трансляцию внешнего WAN IP-адреса модема в IP-адрес Шлюза, который назначен на интерфейсе модема, то «С-Терра Шлюз» может быть только инициатором защищенных/незащищенных соединений.
4. Если дополнительно планируется использовать «С-Терра Шлюз» с модемом для доступа в Интернет, клиентам, располагающимся за криптошлюзом, то на интерфейсе модема настройте NAT при помощи iptables (**Важно:** см. соответствующий пункт документа «Инструкция по настройке NAT и межсетевого экрана на «С-Терра Шлюз» при помощи утилиты «iptables»»).
5. При работе с модемами Huawei Brovi E3372-325 отмечается нестабильность. Достаточно часто возникают отказы при получении адреса по DHCP при загрузке устройства.
6. Если на «С-Терра Шлюз» планируется одновременно использовать два идентичных модема, то для обеспечения нормальной работы убедитесь в том, что выбранная модель позволяет изменять адрес сети, из которой выдается адрес на интерфейс модема. Также для того, чтобы шлюз имел возможность обрабатывать на интерфейсе модема входящие запросы на построение IPsec соединений, выступать в роли ответчика (responder), модем должен поддерживать функции DMZ или Port-Forwarding. Детальнее см. п.3 настоящего раздела.
7. При использовании Mini PCI модема не устанавливайте и не извлекайте SIM-карту при включённом криптошлюзе. Все операции с SIM-картой (установка или извлечение) следует выполнять только при выключенном устройстве.

Особенности использования сервиса резервирования каналов связи MultiWAN

В качестве решения резервирования канала связи используется сервис MultiWAN. Сервис поддерживает использование модема со статической или динамической адресацией. Детальное описание настройки сервиса MultiWAN приведено в документе «Резервирование каналов связи при помощи сервиса MultiWAN».

1. Установите параметр `max_rtt` (время ожидания ICMP-ответа) в файле конфигурации сервиса MultiWAN `/etc/multiwan/config.yaml` на 1000 миллисекунд, чтобы уменьшить вероятность переключения каналов связи при использовании модемов с нестабильным сигналом. Это позволяет реже переключаться с данного канала связи на другой из-за задержек при колебаниях сигнала и потерь пакетов.

   Если при установленном рекомендованном значении параметра `max_rtt` канал связи оказывается недоступным, выполните следующие шаги:

   1.1. Активируйте режим отладки для сервиса MultiWAN, для этого выполните следующую команду:

   ```
   root@sterragate:~# mwan_mgr set --log_level debug
   ```

   1.2. Проанализируйте файл журнала (команда `grep multiwan /var/log/cspvpngate.log`) и на основе полученных данных о времени отклика, при необходимости, увеличьте значение параметра `max_rtt`.

2. Укажите в обязательном параметре `nexthop` в конфигурационном файле сервиса MultiWAN в зависимости от типа адресации модема:

   2.1. Для задания статической адресации укажите IP адрес следующего перехода в обязательном параметре `nexthop` в конфигурационном файле сервиса MultiWAN (IP-адрес, приведенный в примере конфигурационного файла сервиса MultiWAN в п. 3 у интерфейса `usb1`, подойдет для Huawei E3372h-153, для других модемов подсеть может отличаться).

   2.2. Для задания динамической адресации укажите `"DHCP"` в обязательном параметре `nexthop` в конфигурационном файле сервиса MultiWAN.

3. Пример конфигурационного файла `/etc/multiwan/config.yaml` сервиса MultiWAN:

```
config_format_version: 1
links_params:
```

```
links:
- name: ISP1
  iface_name: usb0
  prio: 300
  routes:
    ipv4:
      networks:
      - 0.0.0.0/0
      nexthop: "DHCP"
  check:
    hosts_reachability: any
    ipv4:
      hosts:
      - 1.1.1.1
    method:
      icmp:
        max_rtt: 1000
        interval: 3
        restore_interval: 3
        restore_count: 10
        failure_count: 10
        tos: 184
        data_size: 56
- name: ISP2
  iface_name: usb1
  prio: 200
  routes:
    ipv4:
      networks:
      - 0.0.0.0/0
      nexthop: 192.168.8.1
  check:
    hosts_reachability: any
    ipv4:
      hosts:
      - 8.8.8.8
    method:
      icmp:
        max_rtt: 1000
        interval: 3
        restore_interval: 3
        restore_count: 10
        failure_count: 10
        tos: 184
        data_size: 56
```

4. Если требуется обеспечить резервирование каналов связи и для доступа шлюза в Интернет используются только модемные подключения, то следует использовать модемы разных моделей, которые используют разные сети для интерфейсов модемов, или модемы, которые позволяют изменить сеть по умолчанию.

Предварительные требования

Требования к квалификации администратора

Инженер, планирующий использовать данную инструкцию, должен свободно ориентироваться в настройке базовых сценариев продукта «С-Терра Шлюз» (например, site-to-site IPsec), а также должен знать и понимать следующие технологии и протоколы: PKI, IPsec, NAT, Firewall.

Требования к инфраструктуре

1. Требования к устройствам.

1.1. «С-Терра Шлюз».

1.1.1 Устройство «С-Терра Шлюз» должен быть инициализирован (подробнее на http://doc.s-terra.ru раздел С-Терра Шлюз -> С-Терра Шлюз 5.0 -> «Подключение ПАК и инициализация С-Терра Шлюз на вычислительных системах архитектуры Intel x86-64»).

1.2. Модем.

1.2.1 Модем должен быть заведомо исправен.

1.2.2 В модем должна быть вставлена SIM-карта с возможностью выхода в Интернет.

1.2.3 Если планируете использовать Mini PCI модем в качестве канала связи, то он должен быть подключён к любой свободной PCI шине в выключенном от питания «С-Терра Шлюз», и к модему должны быть подключены антенны для связи.

Добавление модема

Для добавления модема выполните описанные ниже шаги.

1. Подключитесь к локальной консоли разграничения доступа «С-Терра Шлюз» и пройдите процедуру аутентификации (по умолчанию `administrator/s-terra`).
2. Войдите в linux bash:

```
administrator@sterragate] system
Entering system shell...
```

3. Определите какой тип подключения используется для работы с модемом:

3.1. В случае, если используете USB-порт для подключения модема, то подключите USB-модем к любому свободному порту «С-Терра Шлюз» и подождите 30 секунд.

3.2. В случае, если используется шина PCI для подключения модема, то Mini PCI модем уже установлен в «С-Терра Шлюз» в соответствии с п. 1.2.3 раздела «Требования к инфраструктуре».

> При работе с Mini PCI-модемом в случае необходимости установить или извлечь SIM-карту, предварительно выключите криптошлюз.

4. Убедитесь, что в системе появился сетевой интерфейс модема. Сетевой интерфейс модема будет не зарегистрированным и будет без `altname` (в примере `eth3`):

```
root@sterragate:~# ip address show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen
10000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 1c:57:d8:16:0d:22 brd ff:ff:ff:ff:ff:ff
    altname enp1s0
    altname GigabitEthernet0_0
    inet6 fe80::fdd8:f4fa:e50b:3148/64 scope link tentative stable-privacy
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 1c:57:d8:16:0d:23 brd ff:ff:ff:ff:ff:ff
    altname enp2s0
    altname GigabitEthernet0_1
    inet6 fe80::b8ed:c322:a71d:11ff/64 scope link tentative stable-privacy
       valid_lft forever preferred_lft forever
4: eth2: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 1c:57:d8:16:0d:24 brd ff:ff:ff:ff:ff:ff
```

```
    altname enp3s0
    altname GigabitEthernet0_2
    inet6 fe80::935d:8991:73a0:d18/64 scope link tentative stable-privacy
       valid_lft forever preferred_lft forever
5: eth3: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 96:41:65:cb:b9:68 brd ff:ff:ff:ff:ff:ff
```

5. Выполните процедуру регистрации интерфейса модема в Продукте, под именем `usb0`. Для регистрации интерфейса выполните одну из приведенных ниже команд в зависимости от того, какой сетевой интерфейс модема отображается в системе.

   5.1. Если отображается сетевой интерфейс `ethN` (в примере `eth3`), то выполните команду ниже:

   ```
   root@sterragate:~# netifcfg add-device -n usb0 -r eth3
   ```

   ```
   INFO: Renamed interface eth3 to usb0
   INFO: Added new interface 'usb0' with alias 'UsbEthernet0'
   INFO: to both list of persistent ifnames '/etc/netifaces' and list of aliases
   '/etc/ifaliases.cf'
   INFO: Operation completed successfully
   ```

   5.2. Если отображается сетевой интерфейс `usbN` (в примере `usb0`), то выполните команду ниже:

   ```
   root@sterragate:~# netifcfg add-device usb0
   ```

   ```
   INFO: Added new interface 'usb0' with alias 'UsbEthernet0'
   INFO: to both list of persistent ifnames '/etc/netifaces' and list of aliases
   '/etc/ifaliases.cf'
   INFO: Operation completed successfully
   ```

   5.3. Если отображается сетевой интерфейс `wwanN` (в примере `wwan0`), то выполните команду ниже:

   ```
   root@sterragate:~# netifcfg add-device -n usb0 -r wwan0
   ```

   ```
   INFO: Interface wwan0 implements Qualcomm MSM Interface (QMI).
   INFO: It doesn't support automatic configuration and must be
   INFO: configured manually via the command line.
   INFO: Interface will be added, but won't be initialized.
   INFO: Configure it manually or using a script init_qmi_modem.sh
   INFO: Renamed interface wwan0 to usb0
   INFO: Added new interface 'usb0' with alias 'UsbEthernet0'
   INFO: to both list of persistent ifnames '/etc/netifaces' and list of aliases
   '/etc/ifaliases.cf'
   INFO: Operation completed successfully
   ```

   Если сетевой интерфейс модема в системе отображается как `wwanN`, то этот модем использует драйвер `qmi_wwan`. Данный модем является QMI-модемом и требует подготовки к работе. Подробности смотрите в следующем разделе.

   5.4. Если выполнение команды завершилось следующей ошибкой:

   ```
   ERROR: Interface 'wwan0' is not a physical device
   ```

   выполните действия, описанные ниже.

   5.4.1 Проверьте содержимое файла `/sys/class/net/wwan0/qmi/raw_ip`. Если в файле указано значение `Y`, его необходимо изменить на `N`:

   ```
   N
   ```

   Это отключает режим `raw_ip`, который может препятствовать корректной регистрации интерфейса `wwan0`.

   При использовании QMI-модемов на «С-Терра Шлюз» 5.0 и «С-Терра Шлюз» 5.0 BF версий ниже 26871 команду `netifcfg enum` необходимо выполнять до включения интерфейса модема. Если требуется выполнить эту команду во время работы интерфейса модема, его

необходимо предварительно отключить командой `ifdown usb0`, после чего выполнить команду `netifcfg enum`.

5.4.2 После изменения параметра `raw_ip` повторно выполните команду из пункта 5.3.

Примечание. В процессе добавления список интерфейсов, контролируемых драйвером Продукта, будет дополнен именем нового интерфейса, и будет выполнена «привязка» имени интерфейса либо к USB-порту, к которому подключен модем, либо к PCI шине. Таким образом, если после выполнения всех настроек настоящего раздела отключить модем от шлюза, и подключить этот же или другой модем к тому же USB-порту, либо к той же PCI шине, то с этим модемом будет связан интерфейс с присвоенным именем. В данном случае – это `usb0`.

6. Проверьте, что интерфейс успешно добавлен. Для этого выполните команду `netifcfg show`, убедитесь в том, что список интерфейсов дополнен секцией `hotplug` и в этой секции есть имя интерфейса в системе, имя интерфейса в cisco-like консоли:

```
root@sterragate:~# netifcfg show
```

```
INFO: list of persistent ifnames '/etc/netifaces':
pci:
  0000:01:00.0:
    if_name: eth0
    if_alias: GigabitEthernet0/0
  0000:02:00.0:
    if_name: eth1
    if_alias: GigabitEthernet0/1
  0000:03:00.0:
    if_name: eth2
    if_alias: GigabitEthernet0/2
hotplug:
  pci-0000:00:14.0-usb-0:1:1.0:
    if_name: usb0
    if_alias: UsbEthernet0
restricted: {}
INFO: list of aliases '/etc/ifaliases.cf':
GigabitEthernet0/0: eth0
GigabitEthernet0/1: eth1
GigabitEthernet0/2: eth2
default: '*'
UsbEthernet0: usb0
```

7. Убедитесь в том, что системное имя интерфейса модема было корректно изменено. Для этого выполните команду `ip address show`:

```
root@sterragate:~# ip address show
```

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen
10000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 1c:57:d8:16:0d:22 brd ff:ff:ff:ff:ff:ff
    altname enp1s0
    altname GigabitEthernet0_0
    inet6 fe80::fdd8:f4fa:e50b:3148/64 scope link tentative stable-privacy
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 1c:57:d8:16:0d:23 brd ff:ff:ff:ff:ff:ff
    altname enp2s0
    altname GigabitEthernet0_1
    inet6 fe80::b8ed:c322:a71d:11ff/64 scope link tentative stable-privacy
```

```
       valid_lft forever preferred_lft forever
4: eth2: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 1c:57:d8:16:0d:24 brd ff:ff:ff:ff:ff:ff
    altname enp3s0
    altname GigabitEthernet0_2
    inet6 fe80::935d:8991:73a0:d18/64 scope link tentative stable-privacy
       valid_lft forever preferred_lft forever
5: usb0: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 96:41:65:cb:b9:68 brd ff:ff:ff:ff:ff:ff
    altname UsbEthernet0
```

Подготовка к работе QMI-модема

Для работы с QMI-модемами предназначена утилита `qmi_modem`. Она выполняет инициализацию модема перед началом работы с модемом в мобильной сети, а также отключение модема при завершении работы. Ожидается, что утилита `qmi_modem` запускается либо до включения сетевого интерфейса, либо после выключения интерфейса. Параметры для работы с модемом задаются в конфигурационном файле `/etc/stmodems/qmi_modems_conf.yaml`.

Проверьте обязательные параметры конфигурационного файла `/etc/stmodems/qmi_modems_conf.yaml`. Значение параметров `apn`, `apn_user` и `apn_pass` задайте в зависимости от провайдера. Пример конфигурационного файла для провайдера Мегафон:

```
# Файл конфигурации должен быть составлен в соответствии с синтаксисом
# YAML. Файл чувствителен к отступам. Значения чувствительные к реестру.

# "global_parameters" - Содержит глобальные параметры.
# Необязательная секция.
global_parameters:
  # "log_level" - Указывает уровень логирования.
  # Необязательный параметр. Может принимать одно из следующих значений:
  # EMERGENCY, ALERT, CRITICAL, ERROR, WARNING, NOTICE, INFO, DEBUG.
  # Значение по умолчанию: INFO.
  log_level: INFO
  # "log_facility" - Указывает facility.
  # Необязательный параметр. Принимает значения от local0 до local7.
  # Значение по умолчанию: local7.
  log_facility: local7

# "modems" - Используется для указания параметров модемов.
# Обязательный список из секций параметров.
modems:
  - # "iface" - Содержит имя интерфейса в Linux.
    # Обязательный параметр. Значение должно соответствовать шаблону
    # "usbN", где N - число.
    iface: usb0
    # "sim_card" - Содержит параметры для работы сим-карты.
    # Обязательная секция.
    sim_card:
      # "init_try_count" - Указывает количество попыток для проверки
      # доступности сим-карты для работы.
      # Необязательный параметр. Должен быть числом от 1 до 10.
      # Значение по умолчанию: 10.
      init_try_count: 10
      # "init_try_interval" - Указывает интервал между попытками
      # проверки доступности сим-карты для работы.
      # Необязательный параметр. Должен быть числом от 1 до 10.
      # Значение по умолчанию: 3.
      init_try_interval: 3
      # "connection_settings" - Содержит настройки для подключения к
      # мобильному интернету провайдера. Значения нужно узнавать у
      # провайдера. Значения могут отличаться в зависимость от
```

```
      # провайдера.
      # Обязательная секция.
      connection_settings:
        # "apn" - Указывает APN провайдера.
        # Обязательный параметр. Должен быть строкой.
        apn: internet
        # "apn_user" - Указывает имя пользователя.
        # Обязательный параметр. Должен быть строкой.
        apn_user: gdata
        # "apn_pass" - Указывает пароль.
        # Обязательный параметр. Должен быть строкой.
        apn_pass: gdata
        # "ip_type" - Указывает версию протокол APN.
        # Необязательный параметр. Может принимать значение 4 или 6.
        # Значение по умолчанию: 4.
        ip_type: 4
# Пример указания второго модема в modems представлен ниже.
#  - iface: usb1
#    sim_card:
#      init_try_count: 4
#      init_try_interval: 2
#      connection_settings:
#        apn: internet.beeline.ru
#        apn_user: beeline
#        apn_pass: beeline
#        ip_type: 4
```

У некоторых операторов параметры `apn_user` и `apn_pass` не требуются (например, у Tele2). В таком случае их значения оставляют заполненными так, чтобы конфигурация оставалась корректной, например:

```
        apn_user: " "
        apn_pass: " "
```

Настройка сети

Для работы с модемом в мобильной сети необходимо настроить сетевой интерфейс. Существует два варианта его конфигурации:

- Настройка статического IP-адреса – данный вариант настройки подходит для настройки всех модемов, за исключением QMI-модемов.
- Настройка получения IP-адреса по DHCP – универсальный вариант, подходящий для всех модемов.

Примечание. Для QMI-модемов рекомендуется использовать только настройку получения IP-адреса по DHCP, так как IP-адрес выдается провайдером и может меняться в процессе работы. Ручная настройка статического IP может привести к некорректной работе.

1. Для задания статического IP-адреса воспользуйтесь возможностями cisco-like консоли (IP-адрес, приведенный в примерах ниже, подойдет для Huawei E3372h-153, для других модемов подсеть может отличаться):

   1.1. Войдите в консоль cisco-like из linux bash:

   ```
   root@sterragate:~# su cscons
   ```

   1.2. Перейдите в режим настройки:

   ```
   sterragate#configure terminal
   Enter configuration commands, one per line.  End with CNTL/Z.
   ```

   1.3. Задайте IP-адрес 192.168.8.100/24 на интерфейсе `UsbEthernet0` и включите его:

   > Задаваемый, на интерфейс `UsbEthernet0`, IP-адрес должен принадлежать сети модема. IP-адрес сети узнайте в руководстве пользователя или в веб-интерфейсе модема.

```
sterragate(config)#interface UsbEthernet0
sterragate(config-if)#ip address 192.168.8.100 255.255.255.0
sterragate(config-if)#no shutdown
```

1.4. После успешного включения интерфейса `UsbEthernet0` задайте шлюз по умолчанию и IP-адрес DNS-сервера (192.168.8.1 – для Huawei E3372h-153) в cisco-like консоли:

```
sterragate(config)#ip route 0.0.0.0 0.0.0.0 192.168.8.1
sterragate(config)#ip name-server 192.168.8.1
sterragate(config)#end
sterragate#exit
```

1.5. Убедитесь в том, что интерфейс `usb0` запущен и на нем имеется IP-адрес:

```
root@sterragate:~# ip address show usb0
```

```
5: usb0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group
default qlen 1000
    link/ether 96:41:65:cb:b9:68 brd ff:ff:ff:ff:ff:ff
    altname UsbEthernet0
    inet 192.168.8.100/24 brd 192.168.8.255 scope global usb0
       valid_lft forever preferred_lft forever
    inet6 fe80::c401:1c76:f62a:7e02/64 scope link stable-privacy
       valid_lft forever preferred_lft forever
```

2. Для настройки получения IP-адреса по DHCP выполните описанные ниже шаги (**шлюз по умолчанию в cisco-like консоли указывать не нужно, он будет получен по DHCP, либо установлен сервисом MultiWAN, если он используется**).

2.1. Выключите интерфейс:

```
root@sterragate:~# ifdown usb0
```

> Команда `ifdown` нужна для того, чтобы остановить работу интерфейса, однако работает она только с теми интерфейсами, которые описаны в конфигурациях `/etc/network/interfaces`, вне секции, выделенной маркерами `###netifcfg-begin###` - `###netifcfg-end###`, или `/etc/network/interfaces.d/*`. Если интерфейс там не описан, то команда выдаст ошибку `ifdown: interface usb0 not configured` (в таком случае на ошибку можно не обращать внимания).
> Команду `ifdown` следует выполнять перед любым изменением параметров интерфейса в конфигурационных файлах.

2.2. Создайте конфигурационный файл в каталоге `/etc/dhcp/` для сетевого интерфейса. Возьмите содержимое файла из примера `/opt/stmodems/docs/dhclient-usb0.conf.example`. Если интерфейс – `usb0`, назовите файл `dhclient-usb0.conf`:

```
# Configuration file for /sbin/dhclient.
#
# This is a sample configuration file for dhclient. See dhclient.conf's
#       man page for more information about the syntax of this file
#       and a more comprehensive list of the parameters understood by
#       dhclient.
#
# Normally, if the DHCP server provides reasonable information and does
#       not leave anything out (like the domain name, for example), then
#       few changes must be made to this file, if any.
#

option rfc3442-classless-static-routes code 121 = array of unsigned integer 8;

send host-name = gethostname();
request subnet-mask, broadcast-address, time-offset, routers,
        domain-name, domain-name-servers, domain-search, host-name,
        dhcp6.name-servers, dhcp6.domain-search, dhcp6.fqdn, dhcp6.sntp-servers,
```

```
        netbios-name-servers, netbios-scope, interface-mtu,
        rfc3442-classless-static-routes, ntp-servers;

# Required for faster address synchronization when used IP passthrough
send dhcp-lease-time 360;
```

где:

- `send dhcp-lease-time 360;` – команда, указывающая клиенту отправить запрос на аренду IP-адреса с желаемым временем аренды в 360 секунд. Маленькое время аренды позволяет быстрее обновлять адреса, что полезно при использовании сквозного IP-адреса, поскольку это снижает вероятность проблем с задержкой обновления DHCP-параметров.

2.3. Для настройки интерфейса создайте отдельный конфигурационный файл `/etc/network/interfaces.d/usb0` используя один из приведённых ниже вариантов в зависимости от того, используется ли QMI-модем.

2.3.1 Если QMI-модем не используется, в файле `/etc/network/interfaces.d/usb0` укажите следующее содержание конфигурационного файла:

```
auto usb0
allow-hotplug usb0
iface usb0 inet manual
post-up stdhcpclient start -i $IFACE
pre-down stdhcpclient stop -i $IFACE
```

где:

- `auto usb0` – интерфейс будет автоматически активирован при загрузке системы.
- `allow-hotplug usb0` – интерфейс будет включаться при его подключении к системе.
- `iface usb0 inet manual` – создаёт сетевой интерфейс без назначения IP-адреса.
- `post-up stdhcpclient start -i $IFACE` – после включения интерфейса запускается DHCP-клиент для получения IP-адреса. Детальное описание утилиты `stdhcpclient` приведено документе «Сетевые интерфейсы в «С-Терра Шлюз»».
- `pre-down stdhcpclient stop -i $IFACE` – перед отключением интерфейса останавливается DHCP-клиент.

2.3.2 Если используется QMI-модем, файл `/etc/network/interfaces.d/usb0` должен содержать следующую конфигурацию:

```
auto usb0
allow-hotplug usb0
iface usb0 inet manual
pre-up qmi_modem start -i $IFACE
post-up stdhcpclient start -i $IFACE
pre-down stdhcpclient stop -i $IFACE
post-down qmi_modem stop -i $IFACE
```

где:

- `pre-up qmi_modem start -i $IFACE` – перед активацией интерфейса выполняется запуск QMI-модема через утилиту `qmi_modem`.
- `post-down qmi_modem stop -i $IFACE` – после выключения интерфейса модем отключается утилитой qmi_modem.

2.4. Включите интерфейс `usb0` для применения настроек:

```
root@sterragate:~# ifup usb0
```

2.5. Убедитесь, что интерфейс `usb0` запущен, на нём имеется IP-адрес и получено малое время аренды:

```
root@sterragate:~# ip address show usb0
```

```
5: usb0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group
default qlen 10000
```

```
    link/ether 96:41:65:cb:b9:68 brd ff:ff:ff:ff:ff:ff
    altname UsbEthernet0
    inet 192.168.8.119/24 brd 192.168.8.255 scope global dynamic usb0
       valid_lft 358sec preferred_lft 358sec
    inet6 fe80::c401:1c76:f62a:7e02/64 scope link stable-privacy
       valid_lft forever preferred_lft forever
```

Проверка работоспособности

Для проверки работоспособности модема, после успешной регистрации интерфейса модема в Продукте и присвоения на интерфейс IP-адреса, выполните следующие шаги:

1. Определите действующую политику безопасности. Для этого выполните команду `lsp_mgr show`.
2. Если загружена политика драйвера по умолчанию, выполните следующие шаги:

   ```
   root@sterragate:~# lsp_mgr show
   ```

   ```
   Default Driver Policy is loaded
   ```

   2.1. Проверьте, что загруженная политика не блокирует трафик. Для этого выполните команду:

   ```
   root@sterragate:~# dp_mgr show
   ```

   ```
   Default driver policy : passdhcp
   ```

   2.2. Если загружена политика `passdhcp` или `dropall`, то на время проверки загрузите политику `passall`:

   ```
   root@sterragate:~# dp_mgr set -ddp passall
   ```

   ```
   Default driver policy is set successfully
   ```

   2.3. Убедитесь в том, что политика успешно применена:

   ```
   root@sterragate:~# dp_mgr show
   ```

   ```
   Default driver policy : passall
   ```

3. Если применена политика безопасности — убедитесь в том, что к интерфейсу `UsbEthernet0` не примерены списки доступа, блокирующие IPv4 трафик. Для этого в выводе команды `lsp_mgr show` найдите секцию с описанием этого интерфейса и убедитесь в том, что IPv4 трафик не будет блокирован:

   ```
   root@sterragate:~# lsp_mgr show
   ```

   ```
   ...
   NetworkInterface (
       LogicalName = "UsbEthernet0"
       InputFilter = IPv6Default
       OutputFilter = IPv6Default
   )
   ```

4. Убедитесь в том, что доступен какой-либо общедоступный ресурс в сети Интернет, например www.yandex.ru. Для этого выполните команду:

   ```
   root@sterragate:~# ping www.yandex.ru -c 5
   ```

   ```
   PING www.yandex.ru (77.88.55.60) 56(84) bytes of data.
   64 bytes from yandex.ru (77.88.55.60): icmp_seq=1 ttl=55 time=8.45 ms
   64 bytes from yandex.ru (77.88.55.60): icmp_seq=2 ttl=55 time=8.21 ms
   64 bytes from yandex.ru (77.88.55.60): icmp_seq=3 ttl=55 time=9.40 ms
   64 bytes from yandex.ru (77.88.55.60): icmp_seq=4 ttl=55 time=11.0 ms
   64 bytes from yandex.ru (77.88.55.60): icmp_seq=5 ttl=55 time=8.13 ms

   --- www.yandex.ru ping statistics ---
   5 packets transmitted, 5 received, 0% packet loss, time 9ms
   rtt min/avg/max/mdev = 8.128/9.028/10.961/1.066 ms
   ```

5. После завершения проверки верните прежнее значение политики драйвера по умолчанию. Для этого выполните команду `dp_mgr set -ddp <policy>`, где `policy` – имя требуемой политики. Например:

```
root@sterragate:~# dp_mgr set -ddp passdhcp
Default driver policy is set successfully
```

Удаление модема

Перед удалением модема обязательно отмените все настройки (крипто-карты, списки доступа и т.д.), связанные с интерфейсом `UsbEthernet0` из cisco-like консоли или LSP.

1. Выключите интерфейс:

```
root@sterragate:~# ifdown usb0
```

2. Удалите файл `/etc/network/interfaces.d/usb0`.

3. Удалите интерфейс модема из базы Продукта:

```
root@sterragate:~# netifcfg remove-device usb0
INFO: Removed interface 'usb0' from list of aliases '/etc/ifaliases.cf'
INFO: Removed interface 'usb0' from list of persistent ifnames '/etc/netifaces'
INFO: Operation completed successfully
```

4. Убедитесь в том, что интерфейс модема успешно удален. Для этого следует выполнить команду `netifcfg show`. Например:

```
root@sterragate:~# netifcfg show
INFO: list of persistent ifnames '/etc/netifaces':
pci:
  0000:01:00.0:
    if_name: eth0
    if_alias: GigabitEthernet0/0
  0000:02:00.0:
    if_name: eth1
    if_alias: GigabitEthernet0/1
  0000:03:00.0:
    if_name: eth2
    if_alias: GigabitEthernet0/2
hotplug: {}
restricted: {}
INFO: list of aliases '/etc/ifaliases.cf':
GigabitEthernet0/0: eth0
GigabitEthernet0/1: eth1
GigabitEthernet0/2: eth2
default: '*'
```

5. В зависимости от типа подключения выполните следующие действия по извлечению модема:

   5.1. Если модем подключён через USB-порт, то извлеките USB-модем из порта.

   5.2. Если модем подключён через PCI шину, выключите устройство «С-Терра Шлюз», отключите его от питания, затем извлеките Mini PCI-модем из PCI шины.

Приложения

Общие положения

1. Если некоторый USB-модем зарегистрировать под именем `usb0`, а затем:

   - Подключить второй USB-модем (обязательно rndis), система создаст интерфейс с именем `usb1`. Если не добавить второй модем в список обслуживаемых драйвером Продукта и перезагрузить шлюз, интерфейс второго модема получит имя `unknwn_usb0`.

- Отключить модем из текущего USB-порта и подключить его же или другой USB-модем (обязательно rndis) в другой USB-порт, интерфейс будет создан с именем `unknwn_usb0`.

2. Эксплуатировать шлюз в таком состоянии нельзя. В обоих случаях для регистрации интерфейса с именем `unknwn_usb0` выполните команду:

```
root@sterragate:~# netifcfg add-device -n usb1 -r unknwn_usb0
```

```
INFO: Renamed interface unknwn_usb0 to usb1
INFO: Added new interface 'usb1' with alias 'UsbEthernet1'
INFO: to both list of persistent ifnames '/etc/netifaces' and list of aliases
'/etc/ifaliases.cf'
INFO: Operation completed successfully
```

Обновление прошивки модема Huawei Brovi E3372-325

Для обеспечения надежной работы модема Huawei Brovi E3372-325 рекомендуется обновить прошивку. Для обновления прошивки установите в модем SIM-карту, подключите модем к персональному компьютеру под управлением Windows10 или новее. Дождитесь завершения инициализации. Откройте браузер, в адресной строке наберите: http://192.168.8.1. Далее перейдите во вкладку «Дополнительно». На этой вкладке нажмите кнопку «Проверка обновлений». После получения ответа нажмите кнопку «Обновить». Устройство скачает с сайта производителя обновление и применит его.

Во время загрузки и применения обновления модем нельзя отключать от персонального компьютера.

Проверка данных о ПО модема

Проверка данных о ПО QMI-модема проводится для определения совместимости модема с криптошлюзом. Для этого выполните следующие шаги (пример приведён для SIMCom SIM7600E-H):

1. Если используется модем SIMCom SIM7600E-H и есть доступ к модему, отсканируйте QR-код на нём, чтобы получить информацию о ПО и модеме:

```
P/N:S2-10A3Z-Z30H2;SN:MP0623263FDE76E;IMEI:862798068028808;SW:LE20B04SIM7600M22
```

Для модема Quectel EP06-E сканирование QR-кода не может дать информации о ПО, только о модеме.

2. Определите данные о ПО модема с помощью команд:

2.1. Убедитесь, что в системе есть виртуальные последовательные порты `ttyUSB`, с помощью которых осуществляется взаимодействие с модемом. Обычно создаётся до 6 виртуальных устройств:

```
root@sterragate:~# ls /dev/ | grep ttyUSB
```

```
ttyUSB0
ttyUSB1
ttyUSB2
ttyUSB3
ttyUSB4
ttyUSB5
```

Виртуальный последовательный порт `ttyUSB2` используется для отправки AT-команд модему.

2.2. Определите ревизию прошивки с помощью AT команды:

```
root@sterragate:~# echo -n -e "ATI\r\n" > /dev/ttyUSB2 && timeout 1 cat /dev/ttyUSB2
```

```
Manufacturer: SIMCOM INCORPORATED

Model: SIMCOM_SIM7600E-H

Revision: SIM7600M22_V2.0.1

IMEI: 862798068025135
```

```
+GCAP: +CGSM



OK
```

Если команда не выполнилась с первого раза — повторите её. При отсутствии ответа после нескольких попыток используйте другой порт (например, `/dev/ttyUSB3`).

Для модема SIMCom SIM7600E-H дополнительно доступна команда, которая выводит более подробную информацию о ПО:

```
root@sterragate:~# echo -n -e "AT+SIMCOMATI\r\n" > /dev/ttyUSB2 && timeout 1 cat /dev/ttyUSB2
```

```
Manufacturer: SIMCOM INCORPORATED

Model: SIMCOM_SIM7600E-H

Revision: LE20B04SIM7600M22

SIM7600M22_B04V03_210527

QCN:

IMEI: 862798068028808

MEID:

+GCAP: +CGSM

DeviceInfo: 152,170



OK
```

2.3. Определите версию встроенного ПО с помощью AT команды:

```
root@sterragate:~# echo -n -e "AT+CSUB\r\n" > /dev/ttyUSB2 && timeout 1 cat /dev/ttyUSB2
```

```
+CSUB: B04V03

+CSUB: MDM9x07_LE20_S_22_V1.03_210527



OK
```

2.4. Определите версию ПО с помощью команды утилиты `qmicli`:

```
root@sterragate:~# qmicli -d /dev/cdc-wdm0 --dms-get-software-version
```

```
[/dev/cdc-wdm0] Software version: 0.2.c1.7-00091-9607_GENNS_PACK-2
```

где,

- `/dev/cdc-wdm0` – путь к модему.

3. Сопоставьте полученные данные с одним из представленных ниже наборов данных о ПО. Исключением является значение `P/N` для SIMCom SIM7600E-H — его можно не проверять, если отсутствует возможность отсканировать QR-код. Если хотя бы одно из обязательных значений отличается от приведённых поддерживаемых наборов, обратитесь в службу технической поддержки компании для уточнения возможности использования модема.

Поддерживаемые наборы данных о ПО модема SIMCom SIM7600E-H

Производителем проверена поддержка следующих наборов данных о ПО QMI-модема SIMCom SIM7600E-H с «С Терра Шлюз» 5.0.

1. Первый поддерживаемый набор:

   - `Revision: SIM7600M22_V2.0.1;`
   - `Revision: LE20B04SIM7600M22;`
   - `SIM7600M22_B04V03_210527;`
   - `+CSUB: B04V03;`
   - `+CSUB: MDM9x07_LE20_S_22_V1.03_210527;`
   - `Software version: 0.2.c1.7-00091-9607_GENNS_PACK-2;`
   - `P/N:S2-10A3Z-Z30H2.`

   Информацию о `P/N` модема, возможно узнать только отсканировав QR-код нём.

2. Второй поддерживаемый набор:

   - `Revision: SIM7600M22_V1.1;`
   - `Revision: LE11B14SIM7600M22_221022;`
   - `SIM7600M22_LE11_221022_V1.00;`
   - `+CSUB: B14V01;`
   - `+CSUB: MDM9x07_AP_S_22_V1.54_221022;`
   - `Software version: 7_GENNS_PACK-2.510746.2.531259.2;`
   - `P/N:S2-107EQ-Z31FL.`

3. Третий поддерживаемый набор:

   - `Revision: SIM7600M22_V2.0.2;`
   - `Revision: LE20B04SIM7600M22_221130;`
   - `+CSUB: B04V03;`
   - `+CSUB: MDM9x07_LE20_S_22_V1.09_221130;`
   - `Software version: 0.2.c1.7-00138-9607_GENNS_PACK-1;`
   - `P/N:S2-10B47-Z31FJ.`

Поддерживаемые наборы данных о ПО модема Quectel EP06-E

Производителем проверена поддержка следующего набора данных о ПО QMI-модема Quectel EP06-E с «С Терра Шлюз» 5.0.

Поддерживаемый набор:

- `Revision: EP06ELAR04A04M4G;`
- `SubEdition: V04;`
- `Software version: EP06ELAR04A04M4G.`

Критерии определения применимости модемов

1. Проверьте, соответствует ли модем следующим критериям:

   1.1. Подключите модем к шлюзу. Если модем не будет отображаться как новый сетевой интерфейс, значит модем не поддерживается криптошлюзом.

   1.2. Зарегистрируйте новый сетевой интерфейс под именем `usb0`. Модем будет считаться неподдерживаемым криптошлюзом, если вывод команды регистрации будет с ошибкой, например:

   ```
   root@sterragate:~# netifcfg add-device usb0
   ERROR: Interface 'usb0' is not a physical device".
   ```

2. Если модем не указан в списке поддерживаемых или неподдерживаемых устройств и не соответствует ни одному из указанных выше критериев, обратитесь в службу технической поддержки компании для уточнения возможности использования этой модели модема.

Получение доступа к веб-интерфейсу модема

1. Для получения доступа к веб-интерфейсу подключите модем к персональному компьютеру под управлением Windows и дождитесь завершения установки драйверов. После успешной установки браузер по умолчанию автоматически откроет страницу веб-интерфейса модема. Способ применим для модемов Huawei E3372h-153, Huawei E8372h-320.
2. Обратите внимание, что веб-интерфейсы модемов доступны по разным IP-адресам, в зависимости от модели:
   2.1. Alcatel IK41VE1-2AALRU1 – веб-интерфейс доступен по адресу: http://192.168.1.1.
   2.2. Alcatel IK41VE1-2BALRU1 – веб-интерфейс доступен по адресу: http://192.168.1.1.
   2.3. DEXP M1 – веб-интерфейс доступен по адресу: http://192.168.0.1.
   2.4. DEXP M2 – веб-интерфейс доступен по адресу: http://192.168.0.1.
   2.5. Digma Dongle DW1960 – веб-интерфейс доступен по адресу: http://192.168.0.1.
   2.6. Huawei E3372h-607 – веб-интерфейс доступен по адресу: http://192.168.8.1.
   2.7. Huawei Brovi E3372-325 – веб-интерфейс доступен по адресу: http://192.168.8.1.
   2.8. Huawei E3372h-153 – веб-интерфейс доступен по адресу: http://192.168.8.1.
   2.9. Huawei E8372h-320 – веб-интерфейс доступен по адресу: http://192.168.8.1.
   2.10. LTE 4G WIFI Dongle – веб-интерфейс доступен по адресу: http://192.168.100.1.
   2.11. OLAX U90-E – веб-интерфейс доступен по адресу: http://192.168.0.1.
   2.12. Tenda 4G01 – веб-интерфейс доступен по адресу: http://192.168.0.1.
   2.13. ZTE F30 Pro – веб-интерфейс доступен по адресу: http://192.168.0.1.
   2.14. ZTE MF79N – веб-интерфейс доступен по адресу: http://192.168.0.1.
   2.15. ZTE MF79RU – веб-интерфейс доступен по адресу: http://192.168.0.1.
   2.16. ZTE MF833N – веб-интерфейс доступен по адресу: http://192.168.0.1.
   2.17. ZTE MF833T – веб-интерфейс доступен по адресу: http://192.168.0.1.

   Примечание. Установите надежный пароль к веб-интерфейсу.
3. Модем ZTE MF79RU, при подключении к персональному компьютеру под управлением Windows автоматически создает виртуальный CD-ROM. Если драйвера не установились автоматически и не была открыта страница веб-интерфейса запустите установку драйверов вручную, запустив на выполнение файл `AutoRun.exe`, который хранится в корневом каталоге создаваемого CD-ROM.

Тестовый стенд

Тестирование модемов проводилось на стенде, схема которого показана ниже (см. Рисунок 1). Устройство Hub1 защищает подсеть 192.168.100.0/24 и подключено к сети Интернет при помощи статической маршрутизации. Устройство Host-b-hub1 представляет собой персональный компьютер, размещенный в сети, которую защищает Hub1. Устройство Spoke1 защищает подсеть 192.168.1.1/24 и подключено к сети Интернет при помощи модема. Устройство Host-b-spoke1 представляет собой персональный компьютер, размещенный в сети, которую защищает Spoke1. Защищенное соединение строится между устройствами Hub1 и Spoke1. В процессе тестирования осуществляется подключение устройства Spoke1 к сети провайдера по беспроводному каналу и построение защищенного соединения между криптошлюзами. Инициировать построение защищенного соединения возможно только со стороны подсети Spoke1.

Схема стенда

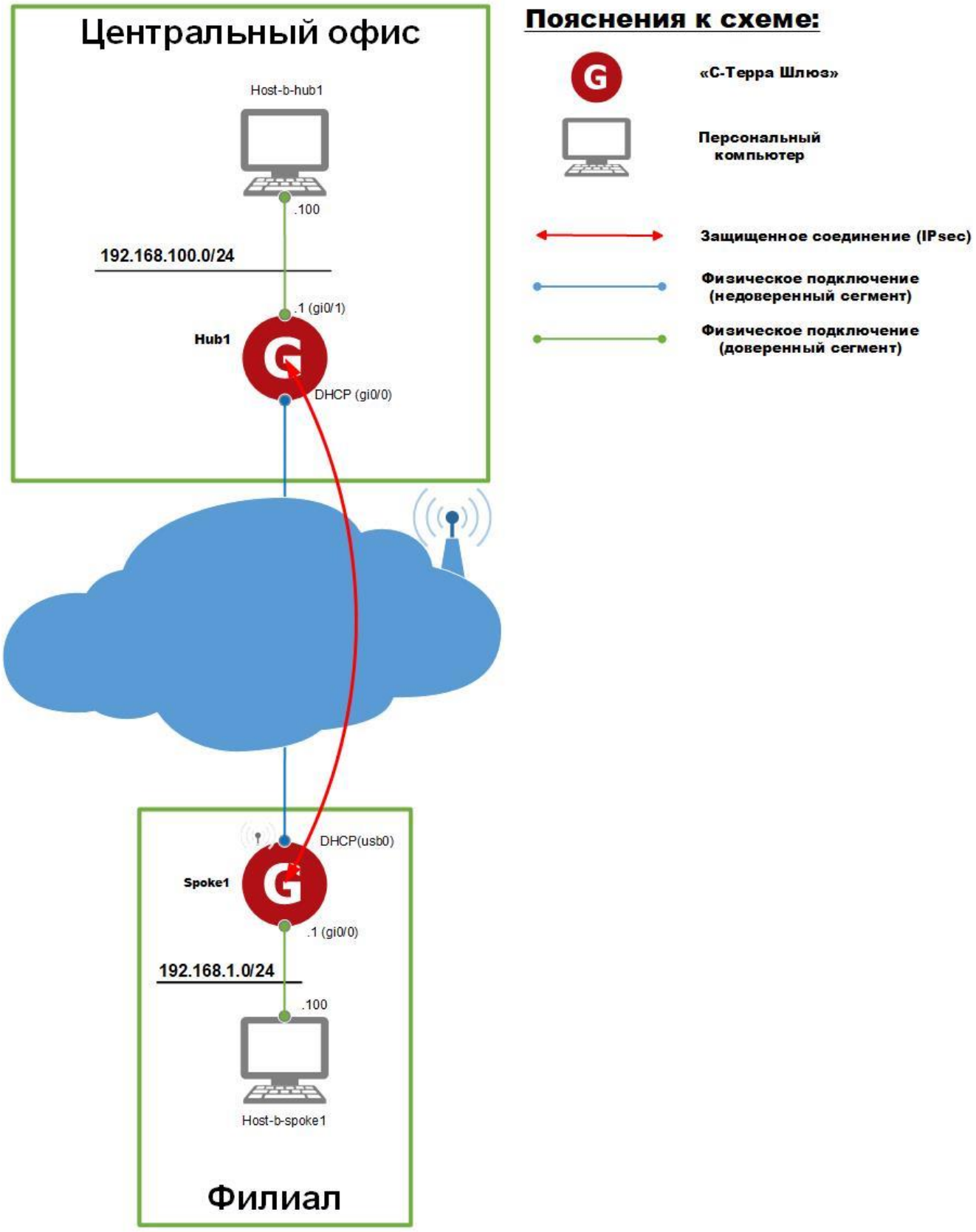


Рисунок 1

Конфигурации устройств

Конфигурация криптошлюза Hub1

1. Консоль cisco-like:

Примечание. Реальный IP-адрес тестового шлюза замаскирован обозначением: XXX.XXX.XXX.XXX.

```
!
version 12.4
no service password-encryption
!
crypto ipsec df-bit copy
crypto isakmp identity dn
crypto isakmp fragmentation
crypto isakmp security-association lifetime delta 50
crypto isakmp initiator-sessions-max 100
crypto isakmp responder-sessions-max 100
crypto ipsec security-association lifetime kilobytes unlimited
crypto isakmp keepalive 3
crypto isakmp keepalive retry-count 5
username           cscons           privilege           15           secret           5
$6$RiWz4IVm$qMp6sbpYnTfSUxuaJPZ9UCq4yy8/xheIEbSmbTfMzmbQqepMD6R1b18vHTdFQt949xNXzpRXW
A9dZ/gCK70z./
aaa new-model
!
!
hostname Hub1
enable secret 5 HGJcyG+CRmCjINGFkW48VQ==
!
!
!
!
!
!
!
crypto isakmp policy 1
 encr magma
 hash stribog-256
 authentication gost-sig
 group vko2
!
crypto isakmp profile NEW_ALGS
 match identity dn
 set identity mapping
 set policy 1
!
crypto ipsec transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY esp-magma-mgm
!
object-group network SELF
 remark WAN IP
 host XXX.XXX.XXX.XXX
!
ip access-list extended IPSEC_ACl_HUB1_AND_SPOKE1
 permit ip 192.168.100.0 0.0.0.255 192.168.1.0 0.0.0.255
!
ip access-list extended FW_INPUT_WAN
 permit udp any object-group SELF eq isakmp
 permit udp any object-group SELF eq non500-isakmp
 permit icmp any object-group SELF
 permit esp any object-group SELF
!
```

```
ipv6 default filtering deny
!
!
ip inspect tcp sessions-max 256000
ip inspect udp sessions-max 65536
ip inspect name INSPECT tcp
ip inspect name INSPECT udp
!
crypto dynamic-map DMAP 1
 match address IPSEC_ACl_HUB1_AND_SPOKE1
 set transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY
 set isakmp-profile NEW_ALGS
 set security-association mss-fix out
 set pre-fragmentation
 set dead-connection history off
!
crypto map VPN 1 ipsec-isakmp dynamic DMAP
!
interface GigabitEthernet0/0
 ip address XXX.XXX.XXX.XXX XXX.XXX.XXX.XXX
 ip access-group FW_INPUT_WAN in
 crypto map VPN
 ip inspect INSPECT out
!
interface GigabitEthernet0/1
 ip address 192.168.100.1 255.255.255.0
!
interface GigabitEthernet0/2
 no ip address
 shutdown
!
!
ip route 0.0.0.0 0.0.0.0 XXX.XXX.XXX.XXX
!
!
crypto pki trustpoint s-terra_technological_trustpoint
 revocation-check none
crypto pki certificate chain s-terra_technological_trustpoint
certificate 58E026BFD6D625BE4582C16C6189C183
30820227308201D4A003020102021058E026BFD6D625BE4582C16C6189C18330
...
AD4F8901771632E0A0AF83

quit
!
end
```

Конфигурации криптошлюза Spoke1

1. Консоль cisco-like:

```
!
version 12.4
no service password-encryption
!
crypto ipsec df-bit copy
crypto isakmp identity dn
crypto isakmp fragmentation
crypto isakmp security-association lifetime delta 50
crypto isakmp initiator-sessions-max 100
crypto isakmp responder-sessions-max 100
crypto isakmp keepalive 3
crypto isakmp keepalive retry-count 5
```

```
username          cscons          privilege          15          secret          5
$6$RiWz4IVm$qMp6sbpYnTfSUxuaJPZ9UCq4yy8/xheIEbSmbTfMzmbQqepMD6R1b18vHTdFQt949xNXzpRXW
A9dZ/gCK70z./
aaa new-model
!
!
hostname Spoke1
enable secret 5 HGJcyG+CRmCjINGFkW48VQ==
!
!
!
!
!
!
!
crypto isakmp policy 1
 encr magma
 hash stribog-256
 authentication gost-sig
 group vko2
!
crypto isakmp profile NEW_ALGS
 match identity dn
 set identity mapping
 set policy 1
!
crypto ipsec transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY esp-magma-mgm
!
object-group network SELF
 remark WAN IP
 10.0.0.0 255.0.0.0
 11.0.0.0 255.0.0.0
 100.0.0.0 255.0.0.0
 192.168.8.0 255.255.255.0
!
ip access-list extended IPSEC_ACl_HUB1_AND_SPOKE1
 permit ip 192.168.1.0 0.0.0.255 192.168.100.0 0.0.0.255
!
ip access-list extended FW_INPUT_WAN
 permit udp any object-group SELF eq isakmp
 permit udp any object-group SELF eq non500-isakmp
 permit icmp any object-group SELF
 permit esp any object-group SELF
 permit udp any eq bootps any eq bootpc
!
ipv6 default filtering deny
!
!
ip inspect tcp sessions-max 256000
ip inspect udp sessions-max 65536
ip inspect name INSPECT tcp
ip inspect name INSPECT udp
!
crypto map VPN 1 ipsec-isakmp
 match address IPSEC_ACl_HUB1_AND_SPOKE1
 set transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY
 set isakmp-profile NEW_ALGS
 set security-association mss-fix out
 set peer XXX.XXX.XXX.XXX
 set pre-fragmentation
 set dead-connection history off
!
```

```
interface GigabitEthernet0/0
 ip address 192.168.1.1 255.255.255.0
!
interface GigabitEthernet0/1
 no ip address
 shutdown
!
interface GigabitEthernet0/2
 no ip address
 shutdown
!
interface UsbEthernet0
 ip address 10.67.7.196 255.255.255.248
 ip access-group FW_INPUT_WAN in
 crypto map VPN
 ip inspect INSPECT out
!
!
!
!
crypto pki trustpoint s-terra_technological_trustpoint
 revocation-check none
crypto pki certificate chain s-terra_technological_trustpoint
certificate 58E026BFD6D625BE4582C16C6189C183
30820227308201D4A003020102021058E026BFD6D625BE4582C16C6189C18330
...
AD4F8901771632E0A0AF83

quit
!
end
```