VPN-туннели

Сервис VPN доступен в Neutron и Sprut SDN. Управление VPN-туннелями в Sprut SDN доступно только через интерфейс личного кабинета.

Вы можете управлять VPN-туннелями: просматривать, добавлять в проект и удалять их из проекта, а также редактировать и перезапускать туннели.

Просмотр списка VPN-туннелей и информации о них

Личный кабинет

1. Перейдите в личный кабинет VK Cloud.
2. Выберите проект.
3. Перейдите в раздел **Виртуальные сети → VPN**.
   Будет отображен список VPN-туннелей.
4. Нажмите на имя VPN-туннеля.
   Откроется страница с подробной информацией о нем. Переходите между вкладками страницы для просмотра информации о параметрах IKE и IPsec, endpoint-групп и туннеля. На этой странице можно также редактировать параметры VPN-туннеля.

OpenStack CLI

1. Убедитесь, что:
   a. OpenStack CLI установлен вместе с дополнительным пакетом python-neutronclient.
   b. Вы можете авторизоваться в OpenStack CLI.
2. Чтобы посмотреть список VPN-туннелей, выполните команду: openstack vpn ipsec site connection list
3. Чтобы посмотреть детальную информацию о VPN-туннеле, выполните команду: openstack vpn ipsec site connection show <идентификатор VPN-туннеля из списка, полученного ранее>

   Будет выведена общая информация о туннеле и идентификаторы:
   - IKE Policy — идентификатор IKE-политики. Чтобы посмотреть детальную информацию о политике, выполните команду: openstack vpn ike policy show <идентификатор IKE-политики>
   - IPSec Policy — идентификатор IPsec-политики. Чтобы посмотреть детальную информацию о политике, выполните команду: openstack vpn ipsec policy show <идентификатор IPsec-политики>
   - Local Endpoint Group ID — идентификатор локальной endpoint-группы. Чтобы посмотреть детальную информацию о группе, выполните команду: openstack vpn endpoint group show <идентификатор локальной endpoint-группы>
   - Peer Endpoint Group ID — идентификатор удаленной (peer) endpoint-группы. Чтобы посмотреть детальную информацию о группе, выполните команду: openstack vpn endpoint group show <идентификатор удаленной endpoint-группы>
   - VPN Service — идентификатор VPN-сервиса, который обслуживает этот VPN-туннель. Чтобы посмотреть детальную информацию о сервисе, выполните команду: openstack vpn service show <идентификатор VPN-сервиса>

Добавление VPN-туннеля

Личный кабинет

1. Перейдите в личный кабинет VK Cloud.
2. Выберите проект.
3. Перейдите в раздел **Виртуальные сети → VPN**.
4. Нажмите кнопку **Добавить VPN** или **Добавить**.
   Откроется мастер создания нового VPN-туннеля.

OpenStack CLI

1. Убедитесь, что:
   a. OpenStack CLI установлен вместе с дополнительным пакетом *python-neutronclient*.
   b. Вы можете авторизоваться в OpenStack CLI.

5. Выберите SDN, в которой будет создан VPN:
   - **SDN Neutron**: VPN можно подключить только к стандартному маршрутизатору Sprut или Neutron.
   - **SDN Sprut**: VPN можно подключить только к продвинутому маршрутизатору.
6. Настройте IKE:
   6.1. **IKE-политика** — выберите IKE-политику из выпадающего списка. Если нужной политики нет, создайте новую:
   6.1.1. Выберите из выпадающего списка пункт *Новая IKE-политика*.
   6.1.2. Задайте настройки политики:
   — **Имя политики**.
   — **Время жизни ключа** (в секундах).
   — **Алгоритм авторизации** — рекомендуется выбрать *sha256*.
   — **Алгоритм шифрования** — рекомендуется выбрать *aes256*.
   — **Версия IKE** — рекомендуется выбрать версию *v2*.
   — **Группа Диффи-Хеллмана** — рекомендуется выбрать группу *group14*.
   6.2. Нажмите кнопку **Следующий шаг**.
7. Настройте IPsec:
   7.1. **IPsec-политика** — выберите IPsec-политику из выпадающего списка. Если нужной политики нет, создайте новую:
   7.1.1. Выберите из выпадающего списка пункт *Новая IPsec-политика*.
   7.1.1. Задайте настройки политики:
   — **Имя политики**.
   — **Время жизни ключа** (в секундах).
   — **Алгоритм авторизации** — рекомендуется выбрать *sha256*.
   — **Алгоритм шифрования** — рекомендуется выбрать *aes256*.
   — **Группа Диффи-Хеллман**а — рекомендуется выбрать группу *group14*.
   7.2. Нажмите кнопку **Следующий шаг**.
8. Настройте endpoint-группы:
   8.1. **Маршрутизатор** — выберите маршрутизатор, подсети которого должны быть доступны через VPN-туннель. Доступные опции зависят от выбранной SDN, и среди них только те маршрутизаторы, которые подключены к внешней сети и имеют назначенный внешний IP-адрес.
   Для одного маршрутизатора рекомендуется создавать не более 500 соединений. При большем количестве соединений могут возникать ошибки.
   8.1. **Local Endpoint** — выберите локальную endpoint-группу из выпадающего списка. Если нужной группы нет, создайте новую:
   8.1.1. Выберите из выпадающего списка пункт *Новая endpoint-группа*.
   8.1.2. Задайте настройки группы:
   Neutron
   — **Имя** — имя локальной endpoint-группы.
   — **Подсети** — выберите одну или несколько подсетей, подключенных к выбранному ранее маршрутизатору. Эти подсети будут доступны через VPN-туннель.
   Sprut
   — **Имя** — имя локальной endpoint-группы.
   — **Адрес подсети** — укажите IP-адрес (CIDR) подсети, подключенной в выбранному ранее маршрутизатору. Эта подсеть будет доступна через VPN-туннель.
   — (Опционально) Для подключения дополнительной подсети нажмите **Добавить еще один CIDR** и укажите IP-адрес подсети, которая должна быть доступна через VPN-туннель.

2. Настройте IKE:
   a. Получите список IKE-политик и посмотрите детальную информацию о политиках:
   openstack vpn ike policy list
   openstack vpn ike policy show <идентификатор политики>
   Запишите идентификатор политики (*id*), которая будет использоваться VPN-туннелем.
   b. Если подходящей IKE-политики на предыдущем шаге не нашлось, создайте ее:
   Linux/macOS (bash, zsh)

```
openstack vpn ike policy create <имя политики> \
  –lifetime units=<единицы измерения, по умолчанию seconds>,value=<время жизни ключа, по умолчанию 3600> \
  –auth-algorithm <Алгоритм авторизации: sha1, sha256> \
  –encryption-algorithm <Алгоритм шифрования: 3des, aes-128, aes-192, aes-256> \
  –ike-version <Версия IKE: v1, v2> \
  –pfs <Группа Диффи-Хеллмана: group5, group2, group14>
```

   Windows (PowerShell)

```
openstack vpn ike policy create <имя политики> `
  –lifetime units=<единицы измерения, по умолчанию seconds>,value=<время жизни ключа, по умолчанию 3600> `
  –auth-algorithm <Алгоритм авторизации: sha1, sha256> `
  –encryption-algorithm <Алгоритм шифрования: 3des, aes-128, aes-192, aes-256> `
  –ike-version <Версия IKE: v1, v2> `
  –pfs <Группа Диффи-Хеллмана: group5, group2, group14>
```

   После создания будет выведена информация о созданном объекте, включающая его идентификатор. Запишите идентификатор политики (*id*), которая будет использоваться VPN-туннелем.
3. Настройте IPsec:
   3.1. Получите список IPsec-политик и посмотрите детальную информацию о политиках:

```
openstack vpn ipsec policy list
openstack vpn ipsec policy show <идентификатор политики>
```

   Запишите идентификатор политики, которая будет использоваться VPN-туннелем.
   3.2. Если подходящей IPsec-политики на предыдущем шаге не нашлось, создайте ее:
   Linux/macOS (bash, zsh)

```
openstack vpn ipsec policy create <имя политики> \
  –lifetime units=<единицы измерения, по умолчанию seconds>,value=<время жизни ключа, по умолчанию 3600> \
  –auth-algorithm <Алгоритм авторизации: sha1, sha256> \
  –encryption-algorithm <Алгоритм шифрования: 3des, aes-128, aes-192, aes-256> \
  –pfs <Группа Диффи-Хеллмана: group5, group2, group14>
```

   Windows (PowerShell)

```
openstack vpn ipsec policy create <имя политики> `
  –lifetime units=<единицы измерения, по умолчанию seconds>,value=<время жизни ключа, по умолчанию 3600> `
  –auth-algorithm <Алгоритм авторизации: sha1, sha256> `
  –encryption-algorithm <Алгоритм шифрования: 3des, aes-128, aes-192, aes-256> `
  –pfs <Группа Диффи-Хеллмана: group5, group2, group14>
```

   После создания будет выведена информация о созданном объекте, включающая его идентификатор. Запишите идентификатор политики, которая будет использоваться VPN-туннелем.
4. Создайте VPN-сервис, который будет обслуживать VPN-туннель:
   4.1. Получите список маршрутизаторов и посмотрите детальную информацию о них:

```
openstack router list
openstack router show <идентификатор маршрутизатора>
```

   Запишите идентификатор маршрутизатора, чьи подсети нужно сделать доступными через VPN-туннель. Такой маршрутизатор должен иметь доступ в интернет и привязанный к нему внешний IP-адрес.

8.2. **Remote Endpoint** — выберите удаленную (remote) endpoint-группу из выпадающего списка. Если нужной группы нет, создайте новую:
8.2.1. Выберите из выпадающего списка пункт *Новая endpoint-группа*.
8.2.2. Задайте настройки группы:
— **Имя группы**.
— **Адрес подсети** — адрес удаленной (remote) подсети, которая будет доступна через VPN-туннель.
При необходимости добавить еще несколько подсетей, нажмите на ссылку **Добавить подсеть**.
8.3. Нажмите кнопку **Следующий шаг**.
9. Настройте VPN-туннель:
9.1. Укажите базовые настройки:
— **Имя туннеля**.
— **Публичный IPv4 адрес пира (Peer IP)**.
— **Ключ совместного использования (PSK)**.
При необходимости сгенерируйте ключ, нажав соответствующую кнопку.
Допустимые символы:
— заглавные и строчные буквы латинского алфавита;
— цифры;
— спецсимволы -, +, &, !, @, #, $, %, ^, *, (,), ,, ., :, ;, _, =, <, >, {, }, /.
Ключ должен содержать хотя бы одну букву или цифру.
9.2. (Опционально) укажите расширенные настройки:
— **Идентификатор маршрутизатора пира для аутентификации (Peer ID)** — по умолчанию совпадает с адресом пира.
— (Только для VPN в SDN Sprut) **Селектор потоков траффика**:
— **Объединить** — не расщеплять трафик-селекторы, то есть оборачивать все адресные префиксы в один туннель передачи данных;
— **Разделить** — расщеплять трафик-селекторы, то есть для каждой пары адресных префиксов создавать отдельный туннель передачи данных.
— **Состояние инициатора** — поведение при установке IPsec-соединения:
— *bi-directional* (по умолчанию) — со стороны платформы VK Cloud будут производиться попытки установления соединения с удаленным пиром (remote peer).
— *response-only* — платформа ожидает, что VPN-соединение будет инициировано удаленным пиром, и не пытается установить его самостоятельно.
— Настройки обнаружения недоступности удаленного пира (Dead Peer Detection, DPD):
— **При обнаружении недоступности пира** — определяет поведение платформы VK Cloud, если удаленный пир недоступен:
— *hold* (по умолчанию) — при обнаружении недоступности IPsec-соединение разрывается. Соединение может быть переустановлено только удаленным пиром.
— *clear* — при обнаружении недоступности IPsec-соединение разрывается. Соединение не будет переустановлено, даже если удаленный пир будет пытаться это сделать.
— *restart* — при обнаружении недоступности IPsec-соединение разрывается. Платформа VK Cloud будет пытаться переустановить соединение с удаленным пиром.
— **Интервал обнаружения недоступности пира** — с каким интервалом (в секундах) отправлять проверочные DPD-сообщения.
— **Время для обнаружения недоступности пира** — если по истечении этого тайм-аута (в секундах) не было получено ни одного проверочного DPD-сообщения от удаленного пира, то он признается недоступным (dead).

4.2. Создайте VPN-сервис, использующий этот маршрутизатор:
Linux/macOS (bash, zsh)

```
openstack vpn service create <имя VPN-сервиса> \
 –router <идентификатор маршрутизатора, полученный на предыдущем шаге> \
 –enable
```

Windows (PowerShell)

```
openstack vpn service create <имя VPN-сервиса> `
 –router <идентификатор маршрутизатора, полученный на предыдущем шаге> `
 –enable
```

После создания будет выведена информация о созданном объекте, включающая его идентификатор. Запишите идентификатор VPN-сервиса, который будет использоваться VPN-туннелем.
5. Настройте endpoint-группы:
5.1. Получите список endpoint-групп и посмотрите детальную информацию о них:

```
openstack vpn endpoint group list
openstack vpn endpoint group show <идентификатор группы>
```

Запишите:
— Идентификатор группы, которая будет использоваться VPN-туннелем в качестве локальной endpoint-группы. Такая группа должна иметь тип subnet.
Подсети, принадлежащие группе, должны быть подключены к маршрутизатору, который указывался на предыдущем шаге в настройках VPN-сервиса.
— Идентификатор группы, которая будет использоваться VPN-туннелем в качестве удаленной endpoint-группы. Такая группа должна иметь тип cidr.
5.2. Если подходящей локальной endpoint-группы не нашлось, создайте ее:

По умолчанию значение этого параметра в четыре раза больше, чем **Интервал обнаружения недоступности пира**.

10. Нажмите кнопку **Создать VPN-туннель**.

1. Убедитесь, что:
   a. OpenStack CLI установлен вместе с дополнительным пакетом python-neutronclient.
   b. Вы можете авторизоваться в OpenStack CLI.
2. Чтобы посмотреть список VPN-туннелей, выполните команду: openstack vpn ipsec site connection list
3. Чтобы посмотреть детальную информацию о VPN-туннеле, выполните команду: openstack vpn ipsec site connection show <идентификатор VPN-туннеля из списка, полученного ранее>

   Будет выведена общая информация о туннеле и идентификаторы:

   - IKE Policy — идентификатор IKE-политики. Чтобы посмотреть детальную информацию о политике, выполните команду: openstack vpn ike policy show <идентификатор IKE-политики>
   - IPSec Policy — идентификатор IPsec-политики. Чтобы посмотреть детальную информацию о политике, выполните команду: openstack vpn ipsec policy show <идентификатор IPsec-политики>
   - Local Endpoint Group ID — идентификатор локальной endpoint-группы. Чтобы посмотреть детальную информацию о группе, выполните команду: openstack vpn endpoint group show <идентификатор локальной endpoint-группы>
   - Peer Endpoint Group ID — идентификатор удаленной (peer) endpoint-группы. Чтобы посмотреть детальную информацию о группе, выполните команду: openstack vpn endpoint group show <идентификатор удаленной endpoint-группы>
   - VPN Service — идентификатор VPN-сервиса, который обслуживает этот VPN-туннель. Чтобы посмотреть детальную информацию о сервисе, выполните команду: openstack vpn service show <идентификатор VPN-сервиса>