Теория.

Виртуальные сети, подсети, IP-адресация

Сети и подсети

Физические серверы в дата-центрах соединяются друг с другом с помощью сети. Виртуальным серверам тоже нужно общаться друг с другом, поэтому для них поверх физической сети построена своя, виртуальная сеть. Она гарантирует, что нужные виртуальные машины смогут передавать данные друг другу, выходить в интернет и подключаться к базам данных, при этом владельцы «соседних» виртуальных машин не смогут увидеть этот трафик или повлиять на него.
Чтобы соединить несколько виртуальных машин, нужно создать облачную сеть. Ресурсы типа виртуальных машин и баз данных, находящиеся в одной облачной сети, по умолчанию «видят» друг друга, а находящиеся в разных сетях — нет. Кроме облачной сети, надо создать ещё и подсети — подмножество сети в конкретной зоне доступности. По умолчанию создаётся по одной подсети для каждой зоны, но вы можете этим управлять, если захотите.

IP-адреса

При создании подсети вы можете выбрать, какие IP-адреса будут выдаваться устройствам в этой подсети. Для этого можно выбрать любой диапазон адресов, вложенный в один из следующих: `10.0.0.0/8`, `172.16.0.0/12` и `192.168.0.0/16`. Это не случайные диапазоны: они зафиксированы в стандарте RFC1918 как немаршрутизируемые в интернете и используются только в локальных сетях.
Стоит учесть, что:

- Допустимая длина префикса варьируется от `/16` до `/28`. Подсеть `10.0.0.0/17` создать можно, а `10.0.0.0/15` или `10.0.0.0/29` — нет.

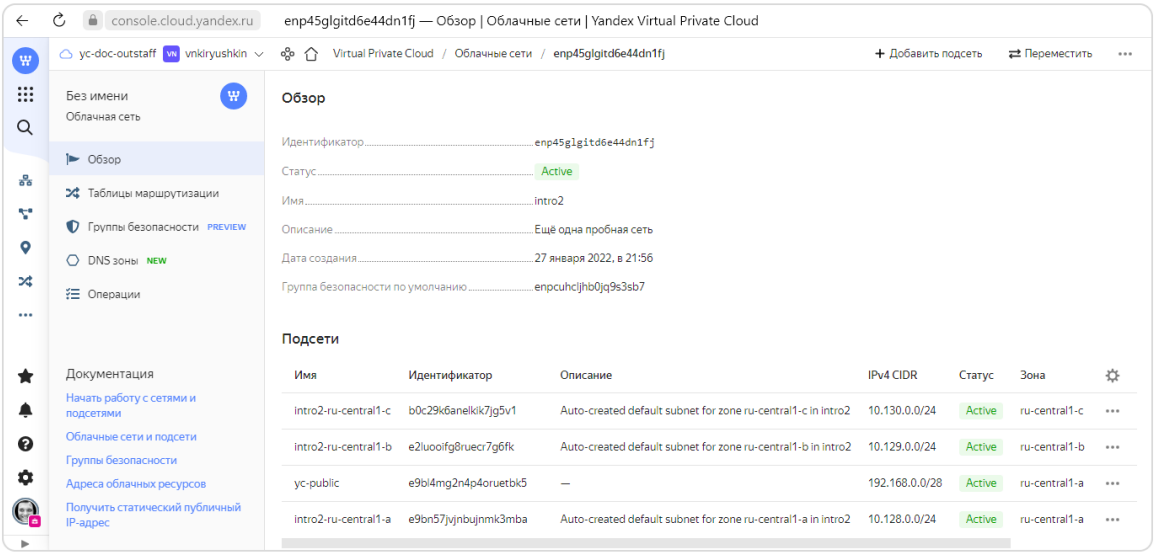
- Первые два адреса подсети выделяются под шлюз (`x.x.x.1` для маски сети `/24`) и DNS-сервер (`x.x.x.2` для маски сети `/24`). Использовать их для виртуальных машин или других ресурсов не получится.
- Внутри одной облачной сети диапазоны IP-адресов всех подсетей не должны пересекаться. В то же время подсети разных облачных сетей могут пересекаться по IP-адресам, ведь две разные сети изолированы друг от друга.
- В Yandex Cloud пока используются только IPv4-адреса. Поддержка IPv6 планируется в будущем.

Внутренние IP-адреса не меняются в течение всего времени существования облачного ресурса. При создании виртуальной машины или другого ресурса их можно задать вручную, или они будут выбраны автоматически в выбранной подсети.
Кроме внутреннего адреса, вы можете выдать виртуальной машине или базе данных также и публичный IP-адрес. Он будет уже принадлежать маршрутизируемому диапазону (например `130.193.32.0/19`), и благодаря этому адресу облачные ресурсы могут обмениваться данными с интернетом и с ресурсами из других облачных сетей. Публичные адреса сопоставляются с внутренними адресами ресурсов с помощью так называемого one-to-one NAT, т. е. одному внешнему адресу соответствует один ресурс в конкретной облачной сети. Подробнее о публичных адресах вы узнаете на одном из следующих уроков.

Практическая работа. Создание новой сети с подсетями и ВМ

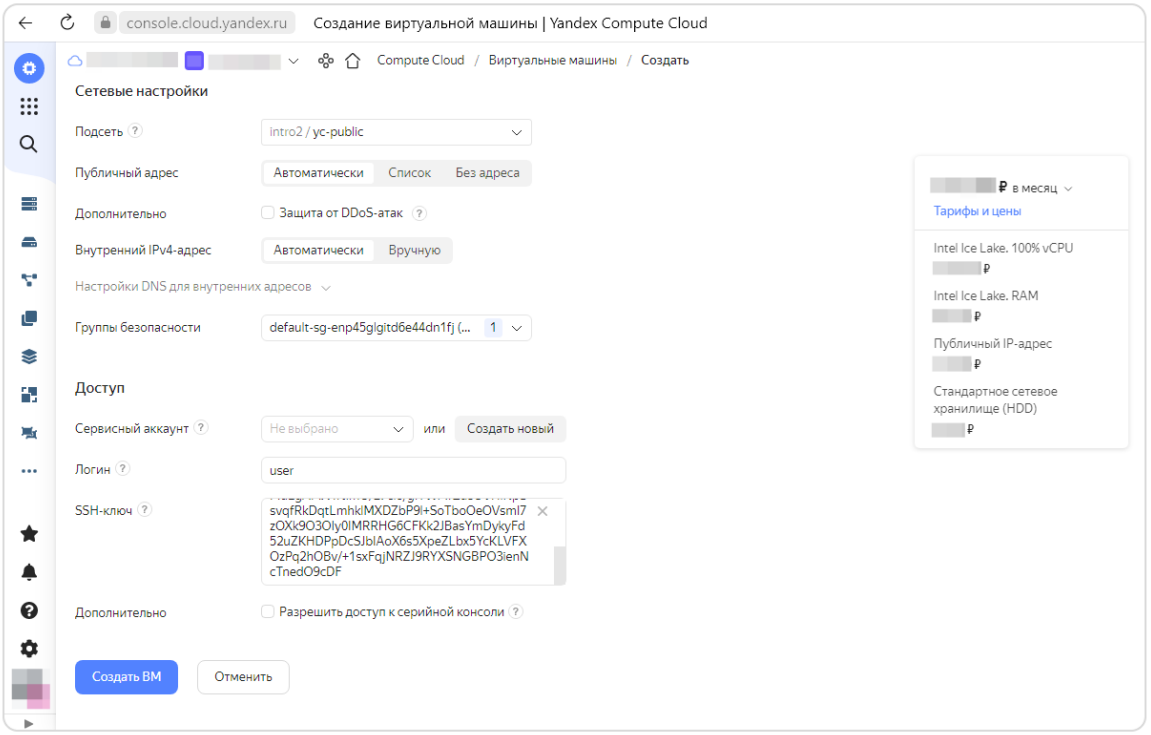
Облачные сети (Virtual Private Cloud, VPC) являются частью публичного облака, которая связывает пользовательские, инфраструктурные, платформенные и прочие ресурсы воедино, где бы они ни находились — в нашем облаке или за его пределами. При этом VPC позволяет не публиковать без необходимости эти ресурсы в интернете, они остаются в пределах вашей изолированной сети.
Когда вы создаёте облако, в нём автоматически появляется сеть и подсети в каждой зоне доступности. Но иногда их бывает недостаточно. На этой практической работе вы научитесь вручную создавать сеть и добавлять подсети.
Рассмотрим пример, как настроить облачную сеть, чтобы организовать работу сервера с доступом из публичной сети. Сначала создадим единую для всех ресурсов облака изолированную сеть с ВМ и другими объектами инфраструктуры.

1. В консоли управления откройте раздел **Virtual Private Cloud** и нажмите кнопку **Создать сеть**. Заполните имя (пусть сеть называется `yc`) и описание. Оставьте выбранной опцию **Создать подсети** и нажмите кнопку **Создать сеть**. В результате появятся три подсети: `yc-ru-central1-a`, `yc-ru-central1-b`, `yc-ru-central1-c`.
2. Для сервера создадим ещё одну подсеть с маской `/28`.
3. В разделе **Virtual Private Cloud** перейдите на страницу сети `yc` и нажмите кнопку **Добавить подсеть**. Введите параметры: имя — `yc-public`, зона — `ru-central-1a`, CIDR — `192.168.0.0/28`. Нажмите кнопку **Создать подсеть**.

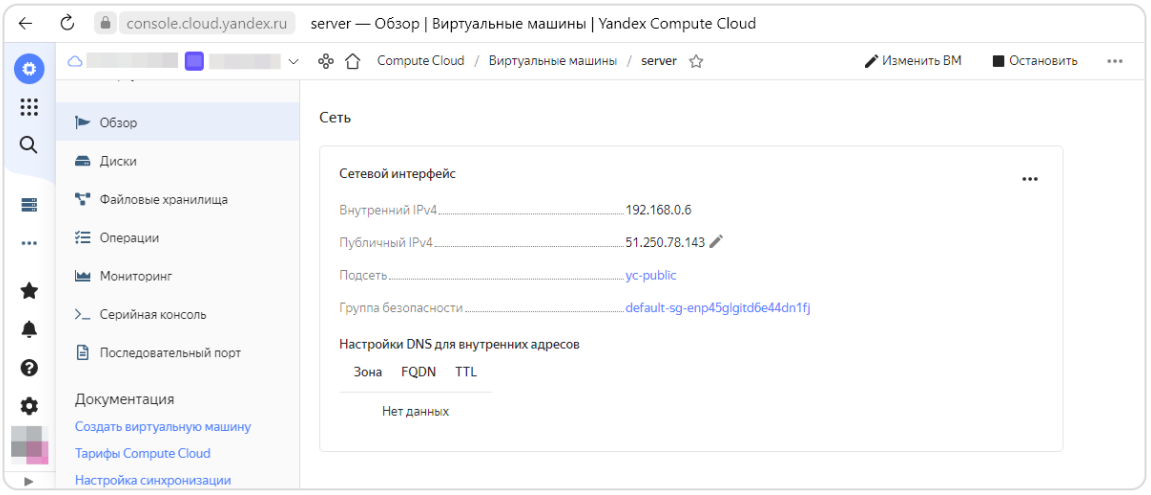


Доступом пользователей облака к сетевым ресурсам управляют с помощью [назначения ролей].

4. Теперь создайте ВМ с именем `server`. Убедитесь, что в блоке **Базовые параметры** выбрана зона доступности `ru-central-1a`. В качестве образа выберите `Ubuntu 20.04`, в блоке **Сетевые настройки** выберите подсеть `yc-public`. В блоке **Доступ** введите логин `user` и вставьте открытый SSH-ключ в соответствующее поле .



После создания ВМ, проверьте доступность сервера, чтобы убедиться, корректно ли настроена сетевая конфигурация. Для этого на странице с информацией о ВМ в блоке **Сеть** найдите публичный IP-адрес сервера:



Откройте интерфейс командной строки и введите команду:
`ping <публичный_ipv4>`

Если конфигурация корректна, в результаты выполнения команды `ping` вы увидите:

```
Ping statistics for 51.250.78.143:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 8ms, Maximum = 9ms, Average = 8ms
```

Такой пример конфигурации подходит для небольшого веб-сервера. Если вы собираетесь строить озеро данных или обрабатывать математические вычисления, не рекомендуется давать к ресурсам прямой доступ из интернета — разместите их за NAT.

Теория.

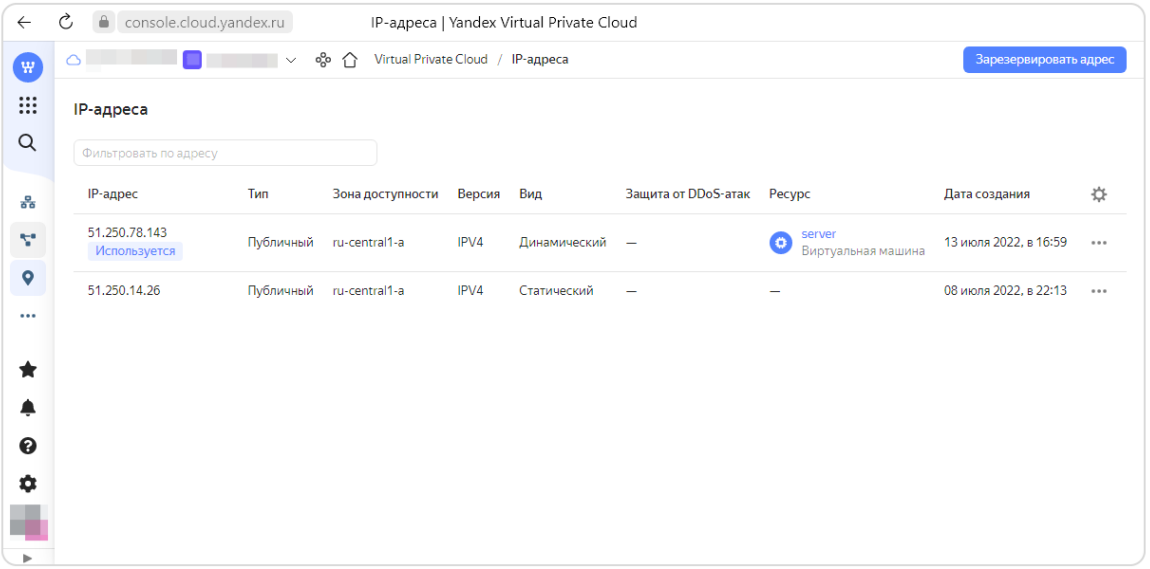
Публичные IP-адреса

Если по внутреннему IP-адресу ВМ доступна только внутри облачной сети, то по публичным IP (они же белые или внешние) она видна и внешнему миру.
Публичный IP-адрес:

- Присваивается по умолчанию при создании облачного ресурса с публичным адресом, если выставлены соответствующие настройки.
- По умолчанию динамический (каждый раз новый при запуске ресурса), но его можно сделать статическим.

Динамические IP-адреса освобождаются при остановке ресурса и сохраняются при перезагрузке. Статические IP сохраняются при остановке ресурса. Их можно зарезервировать и использовать позже, даже если они не привязаны к ресурсу.
Публичные IP-адреса с ресурсами, к которым они привязаны, перечислены в консоли управления в разделе **Virtual Private Cloud** на вкладке **IP-адреса**. Эта вкладка доступна в двух случаях:

1. У вас есть ВМ с публичными адресами.
2. У вас есть статические публичные IP-адреса.



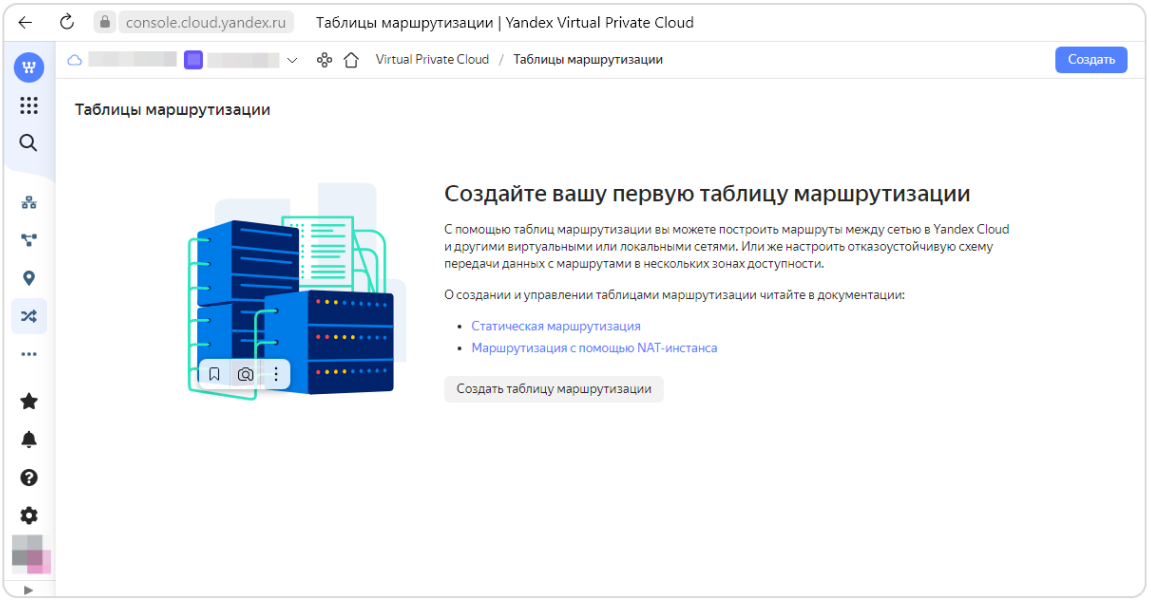
Если вы остановите и снова запустите ВМ, вы увидите, что её публичный IP-адрес изменился.
Чтобы на ВМ работал сервис, постоянно доступный по одному и тому же публичному IP-адресу, поменяйте динамический IP на статический:

1. В списке публичных IP-адресов найдите адрес нужной ВМ.
2. Справа нажмите . . . и в раскрывшемся списке выберите **Сделать статическим**.
3. Остановите и снова запустите ВМ. Вы увидите, что публичный IP-адрес остался прежним.

Статическая маршрутизация

С помощью статической маршрутизации вы можете направлять трафик из подсети на заданные диапазоны IP-адресов через ВМ, указанные в качестве шлюза (next hop). Для этого используются таблицы маршрутизации. Они содержат статические маршруты, состоящие из префикса целевой подсети в нотации CIDR и внутреннего IP-адреса шлюза.

Чтобы создать таблицу маршрутизации со статическим маршрутом, в консоли управления в разделе **Virtual Private Cloud** перейдите на страницу облачной сети, слева выберите вкладку **Таблицы маршрутизации** и нажмите кнопку **Создать таблицу маршрутизации**.



Укажите название таблицы, добавьте статический маршрут и нажмите кнопку **Создать таблицу маршрутизации**.

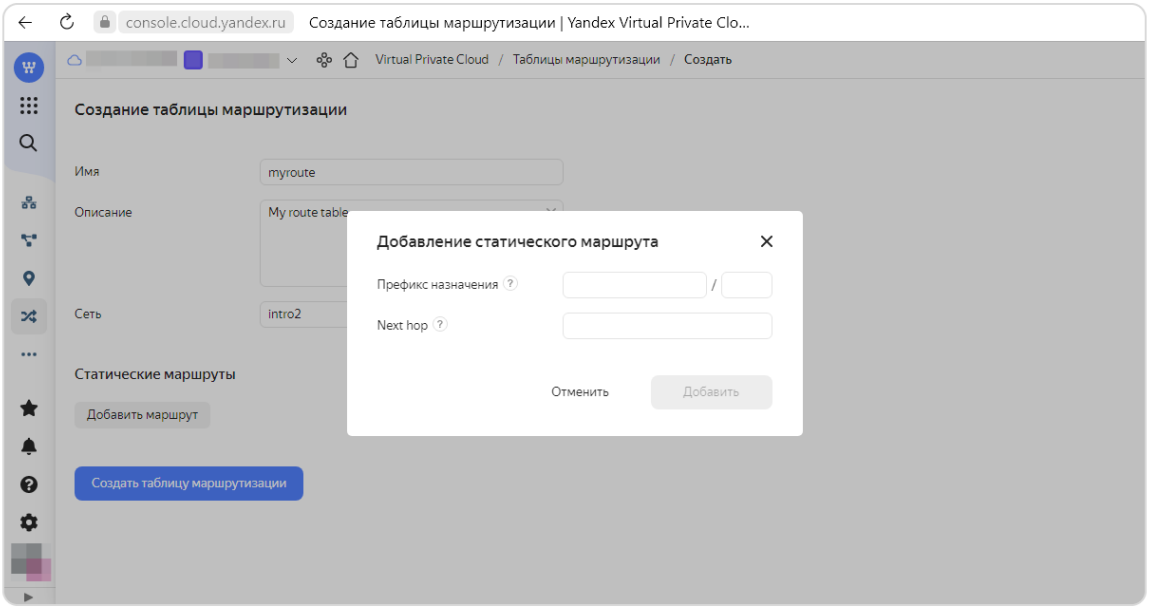


Таблица маршрутизации привязывается к подсети и не может содержать повторяющихся префиксов. Трафик из подсети с привязанной таблицей будет направляться к указанным в маршрутах префиксам через соответствующий адрес шлюза.
Префикс `0.0.0.0/0` в маршруте означает, что весь трафик, если он не направлен по другим маршрутам, будет направлен через указанный для этого префикса шлюз.
Например, к подсети с CIDR `10.1.0.0/24` привязана таблица маршрутизации с такими маршрутами:

Имя	Префикс	Шлюз
another-network	192.168.0.0/16	10.1.0.5
internet	0.0.0.0/0	10.1.0.10

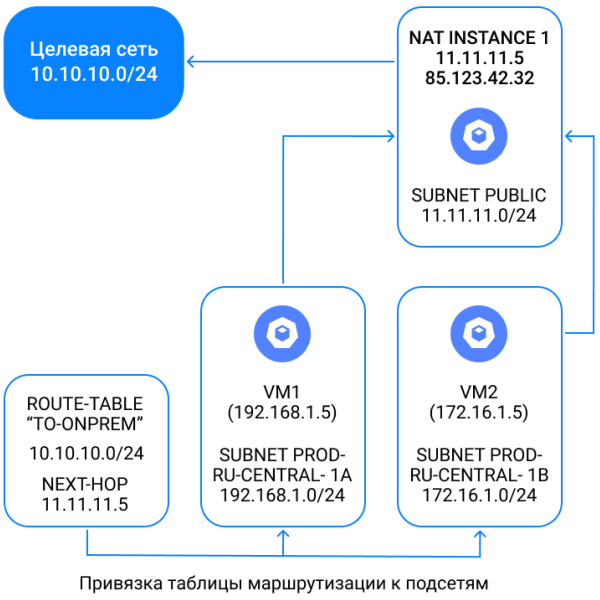
В этом случае весь трафик в подсеть `192.168.0.0/16`, которая находится в другой виртуальной сети, будет направляться через ВМ с адресом `10.1.0.5` — при условии, что у ВМ есть интерфейс в другой виртуальной сети. Весь остальной трафик — через ВМ `10.1.0.10`. При этом переопределение маршрута для префикса `0.0.0.0/0` может повлиять на внешнюю доступность ВМ из подсети с таблицей, где есть такой маршрут.

В Yandex Cloud поддерживаются только префиксы назначения вне виртуальной сети (например, префиксы подсетей другой сети Yandex Cloud или вашей локальной сети).
При создании маршрута в качестве шлюза можно указать свободный внутренний IP-адрес, который не привязан ни к одной ВМ. В этом случае маршрут заработает, когда будет запущена ВМ с соответствующим IP-адресом.

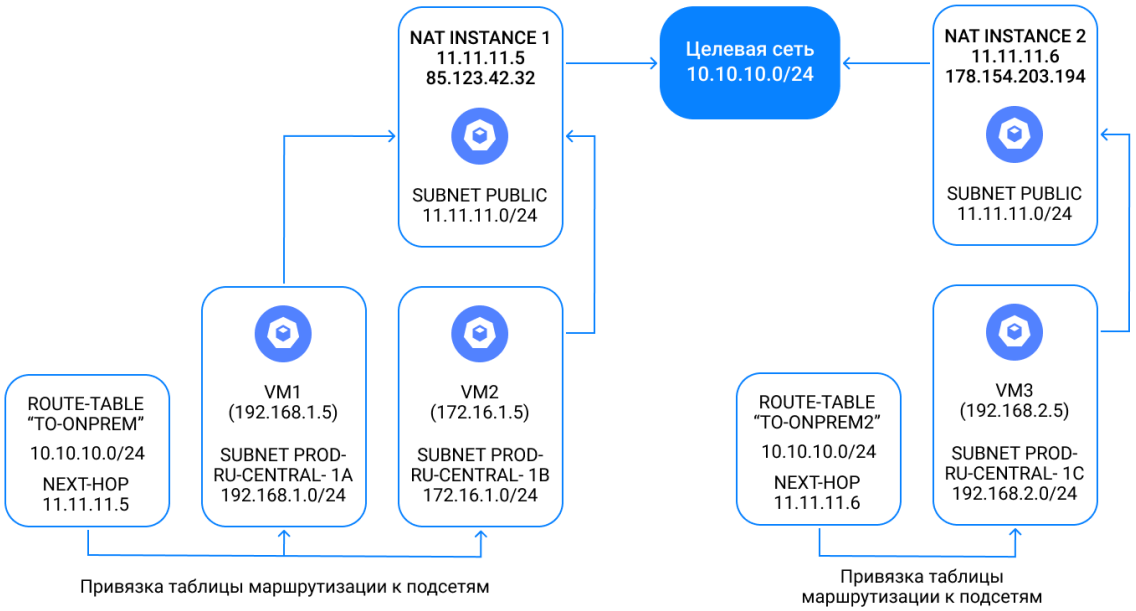
Для чего используются статические маршруты

Есть две типичные схемы использования статических маршрутов в Yandex Cloud:

1. Сетевой маршрут строится до нужного префикса через одну ВМ. В качестве шлюза используется внутренний IP-адрес NAT INSTANCE 1.



2. Отказоустойчивая схема с маршрутами в нескольких зонах доступности. Создайте ВМ в разных зонах доступности и проложите через них маршруты до одной подсети назначения. Если ВМ в одной зоне выйдет из строя — у ВМ из других зон сохранится связность с подсетью назначения.



Изменение маршрутов трафика в интернет

Если в префиксе назначения у маршрута из таблицы маршрутизации указан префикс адресов из интернета, то доступ к таким адресам и с таких адресов станет невозможным через публичные IP-адреса ВМ из подсетей, к которым привязана эта таблица.
Допустим, есть машина `vm-1` с публичным IP-адресом, подключенная к подсети `my-subnet`. Если к подсети `my-subnet` привязать таблицу `my-route-table` с маршрутом для префикса `0.0.0.0/0` (все адреса) через шлюз `10.0.0.5`, то доступ через публичный адрес к `vm-1` пропадёт. Это произойдёт потому, что весь трафик в подсеть `my-subnet` и из неё теперь будет направляться через адрес шлюза (см. первую схему).
Чтобы сохранить входящую связность с облачными ресурсами через публичный адрес, вы можете:

- вынести ресурсы с публичными адресами в отдельную подсеть;
- вместо настройки маршрута в интернет включить для подсети доступ в интернет через NAT (функция находится на стадии Preview и включается по запросу в техподдержку).