

Cats in the Clouds

В качестве выполнения задания был заведен аккаунт у Google Cloud Platform.

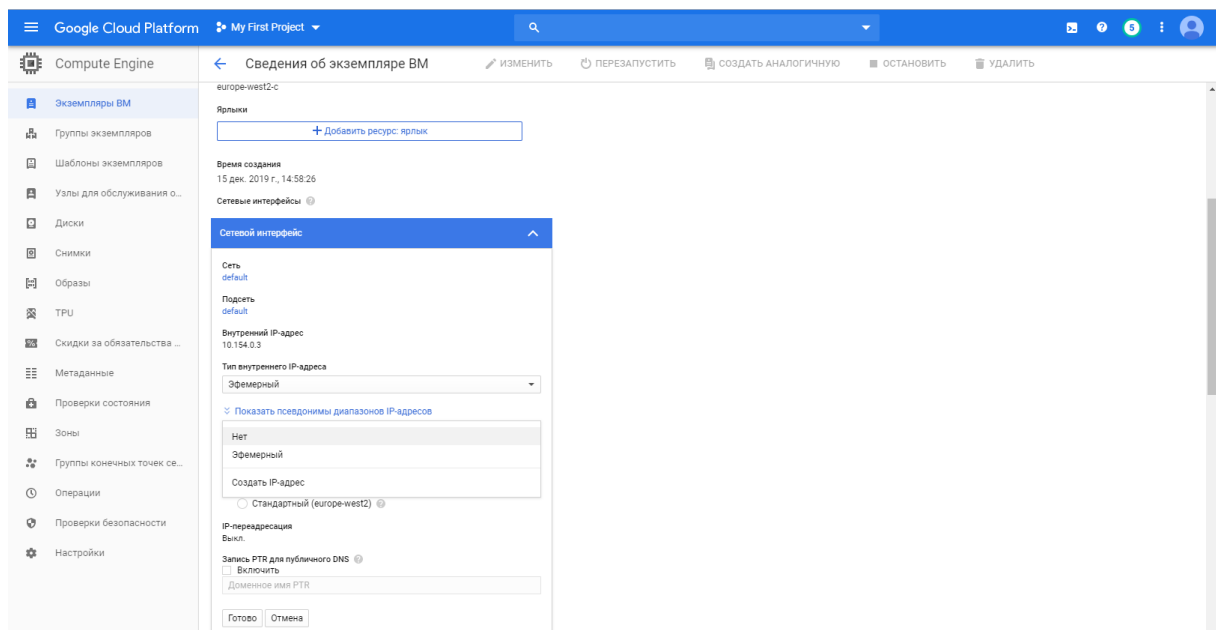
Дальше я сначала опишу, как серверы из задания создаются, а потом уже – как на них можно зайти.

1 Создание

Для начала создадим машины (инстансы): 2 штуки для двух web-серверов (внешний и внутренний соответственно). Это делается на вкладке "Экземпляры ВМ". В самом начале работы список пустой, так что можем добавлять инстансы по своему усмотрению.

1. Внешний: зона Лондон (europe-west2-c), также выбрала ubuntu-1804 (в основном, основываясь на [видео-уроке](#)).
2. Внутренний: тоже зона Лондон (europe-west2-c), также выбрала ubuntu-1804.

Однако тут после создания зайдём в настройки и поменяем тип внешнего IP-адреса со значения "эфемерный" на "нет". То есть, это будет внутренний сервер без имеющегося внешнего IP-адреса:



Как можно заметить, на вкладке "Экземпляры ВМ" появилось 2 инстанса: один с имеющимся внешним IP-адресом, а второй – без него:

Google Cloud Platform

My First Project

Compute Engine

Экземпляры VM

СОЗДАТЬ ЭКЗЕМПЛЯР

ИМПОРТИРОВАТЬ VM

ОБНОВИТЬ

ЗАПУСТИТЬ

ПОКАЗАТЬ ИНФОРМАЦИОННУЮ ПАНЕЛЬ

Экземпляры VM

Группы экземпляров

Шаблоны экземпляров

Узлы для обслуживания о...

Диски

Снимки

Образы

TPU

Скидки за обязательства ...

Метаданные

Проверки состояния

Зоны

Группы конечных точек се...

Операции

Проверки безопасности

Настройки

Введите фильтр

Столбцы

Название	Зона	Рекомендация	Используется	Внутренний IP-адрес	Внешний IP-адрес	Подключиться
gcloud-instance-ellen1	europa-west2-c			10.154.0.2 (nic0)	35.197.192.169	SSH
gcloud-instance-ellen2	europa-west2-c			10.154.0.3 (nic0)	Не задан	SSH

Теперь переходим на Сеть -> Сеть VPC -> Сети VPC, чтобы создать свою виртуальную сеть. Изначально там 20 дефолтных подсетей.

Google Cloud Platform

My First Project

Сеть VPC

Сети VPC

СОЗДАТЬ СЕТЬ VPC

ОБНОВИТЬ

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена трафиком V...

Общая сеть VPC

Бескверный доступ к VPC

Зеркалирование пакетов

Название	Регион	Подсети	Режим	Диапазоны IP-адресов	Шлюзы	Правила брандмауэра	Глобальная динамическая маршрутизация	Журналы логов
default		20	Автоматический		4		Вкл.	
us-central1	default			10.128.0.0/20	10.128.0.1		Вкл.	
europa-west1	default			10.132.0.0/20	10.132.0.1		Вкл.	
us-west1	default			10.138.0.0/20	10.138.0.1		Вкл.	
asia-east1	default			10.140.0.0/20	10.140.0.1		Вкл.	
us-east1	default			10.142.0.0/20	10.142.0.1		Вкл.	
asia-northeast1	default			10.146.0.0/20	10.146.0.1		Вкл.	
asia-southeast1	default			10.148.0.0/20	10.148.0.1		Вкл.	
us-east4	default			10.150.0.0/20	10.150.0.1		Вкл.	
australia-southeast1	default			10.152.0.0/20	10.152.0.1		Вкл.	
europa-west2	default			10.154.0.0/20	10.154.0.1		Вкл.	
europa-west3	default			10.156.0.0/20	10.156.0.1		Вкл.	
southamerica-east1	default			10.158.0.0/20	10.158.0.1		Вкл.	
asia-south1	default			10.160.0.0/20	10.160.0.1		Вкл.	
northamerica-northeast1	default			10.162.0.0/20	10.162.0.1		Вкл.	
europa-west4	default			10.164.0.0/20	10.164.0.1		Вкл.	
europa-north1	default			10.166.0.0/20	10.166.0.1		Вкл.	
us-west2	default			10.168.0.0/20	10.168.0.1		Вкл.	
asia-east2	default			10.170.0.0/20	10.170.0.1		Вкл.	
europa-west5	default			10.172.0.0/20	10.172.0.1		Вкл.	
asia-northeast2	default			10.174.0.0/20	10.174.0.1		Вкл.	

Создаем новую сеть "mycatnet" и для нее подсеть "mycatnet1":

Теперь перейдем в раздел "Правила брандмауэра".

Создаем новое правило, например "rulecat":

Тут сеть выбираем уже не default, а нашу созданную "mucatnet".

Почти всем полям оставляю значения по умолчанию, в том числе приоритет = 1000, а диапазоны IP-адресов источников оставим 0.0.0.0/0.

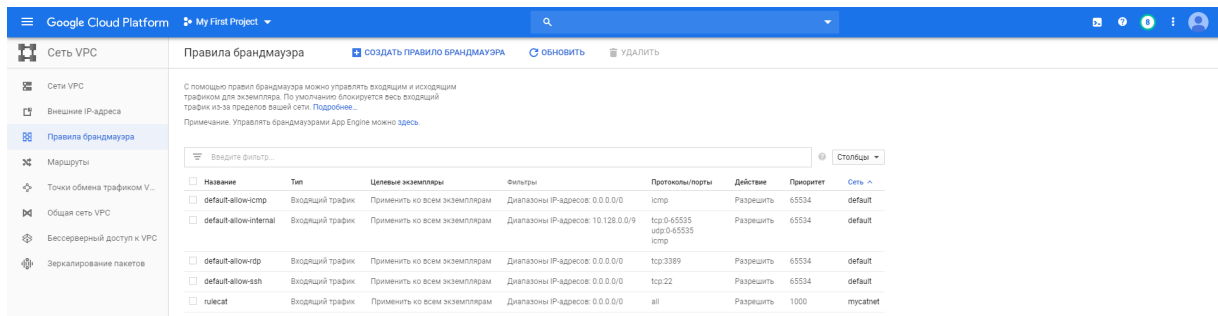
И, самое главное, там где "протоколы и порты", жмем "разрешить все":

Протоколы и порты ?
☒ Разрешить все
☐ Указанные протоколы и порты

⌵ Отключить правило

Создать Отмена

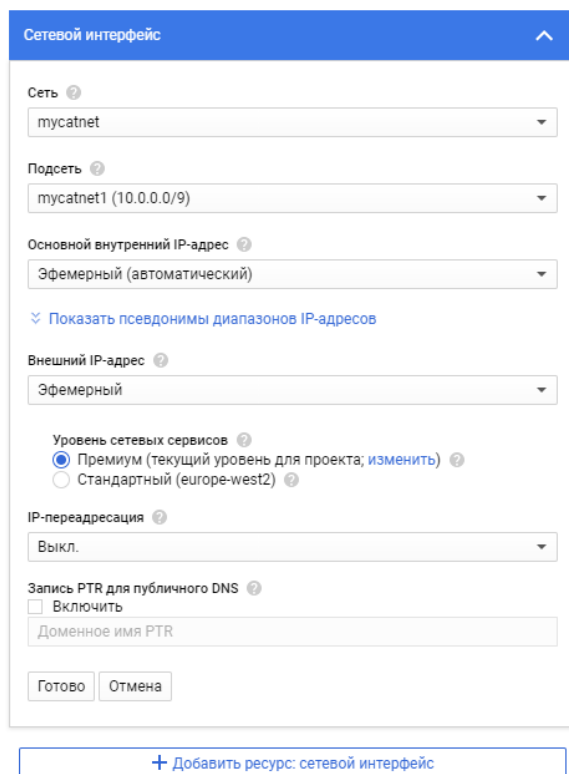
После создания правило появится в списке:



The screenshot shows the Google Cloud Platform console for a project named 'My First Project'. The left sidebar shows the navigation menu with 'Правила брандмауэра' (Firewall Rules) selected. The main content area displays a table of firewall rules. The table has columns: 'Название' (Name), 'Тип' (Type), 'Целевые экземпляры' (Target instances), 'Фильтры' (Filters), 'Протоколы/порты' (Protocols/ports), 'Действие' (Action), 'Приоритет' (Priority), and 'Сеть' (Network). There are four rules listed: 'default-allow-icmp', 'default-allow-internal', 'default-allow-rdp', and 'rulecat'. The 'rulecat' rule is highlighted.

Название	Тип	Целевые экземпляры	Фильтры	Протоколы/порты	Действие	Приоритет	Сеть
default-allow-icmp	Входящий трафик	Применить ко всем экземплярам	Диапазоны IP-адресов: 0.0.0.0/0	icmp	Разрешить	65534	default
default-allow-internal	Входящий трафик	Применить ко всем экземплярам	Диапазоны IP-адресов: 10.128.0.0/9	tcp:0-65535 udp:0-65535 icmp	Разрешить	65534	default
default-allow-rdp	Входящий трафик	Применить ко всем экземплярам	Диапазоны IP-адресов: 0.0.0.0/0	tcp:3389	Разрешить	65534	default
default-allow-ssh	Входящий трафик	Применить ко всем экземплярам	Диапазоны IP-адресов: 0.0.0.0/0	tcp:22	Разрешить	65534	default
rulecat	Входящий трафик	Применить ко всем экземплярам	Диапазоны IP-адресов: 0.0.0.0/0	all	Разрешить	1000	mycatnet

Теперь снова перейдем на Compute Engine -> Экземпляры ВМ, где для двух инстансов поменяем сеть с дефолтной на только что созданную. Оказалось, что это сделать уже нельзя, так что я создам два новых инстанса, сразу указав в поле "Сетевые интерфейсы" нужное значение:



The screenshot shows the 'Сетевой интерфейс' (Network Interface) configuration form in the Google Cloud Platform console. The form has a blue header with the title 'Сетевой интерфейс'. The fields are: 'Сеть' (Network) set to 'mycatnet', 'Подсеть' (Subnet) set to 'mycatnet1 (10.0.0.0/9)', 'Основной внутренний IP-адрес' (Primary internal IP address) set to 'Эфемерный (автоматический)' (Ephemeral (automatic)), 'Внешний IP-адрес' (External IP address) set to 'Эфемерный' (Ephemeral), 'Уровень сетевых сервисов' (Network service level) with 'Премиум (текущий уровень для проекта; изменить)' (Premium (current level for project; change)) selected, 'IP-перенадресация' (IP forwarding) set to 'Выкл.' (Off), and 'Запись PTR для публичного DNS' (PTR record for public DNS) with 'Включить' (On) selected. At the bottom, there are 'Готово' (Done) and 'Отмена' (Cancel) buttons, and a link to '+ Добавить ресурс: сетевой интерфейс' (+ Add resource: network interface).

И сразу разрешу на всякий случай трафик HTTP и HTTPS.

Брандмауэр ?

Чтобы разрешить определенный трафик из Интернета, добавьте теги и правила брандмауэра.

- ☒ Разрешить трафик HTTP
- ☒ Разрешить трафик HTTPS

Первый инстанс "catserver1" будем внешним, а второй "catserver2" - внутренним (подробнее про внешний IP см. в начале).

Сетевые интерфейсы								
Название	Сеть	Подсеть	Основной внутренний IP-адрес	Псевдонимы диапазонов IP-адресов	Внешний IP-адрес	Уровень сети ?	IP-переедресация	Сведения о сети
nic0	mycatnet	mycatnet1	10.0.0.3	—	Не задан		Выкл.	Подробнее...

Брандмауэры

- ☒ Разрешить трафик HTTP
- ☒ Разрешить трафик HTTPS

Теперь настроим NAT.

Для этого переходим в Сетевые сервисы -> Cloud NAT.

Создаем новый NAT-шлюз для нашей сети:

The screenshot shows the Google Cloud Platform console interface. The left sidebar lists network services, with 'Cloud NAT' selected. The main panel displays the configuration for a NAT gateway named 'catnat1'. The status is 'Выполняется' (Running). The configuration includes:

- Маршрутизатор Cloud Router:** Region: europe-west2, VPC: mycatnet, Cloud Router: catrouter.
- Сопоставление NAT:** High availability: Да (Yes). Source IP ranges: Имя подсети (Subnet name) and IP-адреса NAT (NAT IP addresses). A button 'Выделить автоматически' (Select automatically) is present.
- Расширенные настройки (Advanced settings):**
 - Минимальное количество портов на экземпляр VM: 64
 - Время ожидания подключения по протоколу: UDP (30 сек), Session TCP завершен (1200 сек), Промежуточный TCP (30 сек), ICMP (30 сек).
 - Stackdriver Logging: Без журнала (No logs).

Кроме того, мы в ходе создания NAT-шлюза создали и маршрутизатор:

Создание маршрутизатора

Маршрутизатор Google Cloud Router динамически передает данные о маршрутах из виртуального частного облака (VPC) в локальные сети и обратно по протоколу BGP.

Название

Название нельзя будет изменить.

Описание (Необязательно)

Сеть

Регион

Регион нельзя будет изменить.

Теперь настроим DNS.

Для этого переходим в Сетевые сервисы -> Cloud DNS.

Создание (с той информацией, которую надо ввести) на картинке:

← Создание DNS-зоны

DNS-зона служит контейнером для записей DNS с одинаковым суффиксом DNS-имени. В Cloud DNS все записи, относящиеся к управляемой зоне, хранятся на принадлежащих Google авторитетных серверах доменных имен одной группы. [Подробнее...](#)

Вы можете купить домен через [Google Domains](#).

Тип зоны

- ☒ Частная
☐ Публичная

Название зоны

DNS-имя

Описание (Необязательно)

Параметры

Сети (Необязательно)

Частная зона будет доступна в выбранных сетях

- default
✓ mycatnet

Эквивалентный [запрос/ответ REST](#) или команда `gcloud`

Кроме того, для внутреннего инстанса (там внутренний IP равен 10.0.0.3) создаем (нам нужен доступ к нашему внутреннему сайту):

← Изменение набора записей

DNS-имя ?
internalcat.my.dns.cat.example.

Тип записи ресурса ?
A

Время жизни ?
2

Единица ?
недели

Адрес IPv4 ?
10.0.0.3

+ Добавить

Сохранить Отмена

Эквивалентный запрос/ответ REST или команда gcloud

Теперь создадим веб-страницы, установив web-серверы.

Заходим в Экземпляры ВМ и нажимаем на **SSH** напротив нужного инстанса (начнет с первого, для которого создаем внешний сервер).

Далее пользовалась в основном статьей [этой](#). Как раз для этой части мы ранее и настраивали правила брандмауэра.

Итак, выполним команду:

```
1 sudo apt-get update && sudo apt-get install apache2 -y
```

Далее, на предыдущем сайте не указано, но сказано [тут](#):

```
1 sudo apt-get install apache2 vim
```

Теперь можно прописать, например, в таком виде:

```
1 echo '<!doctype html> <html> <body> <h1>SBT Networks 2019 External</h1> <h3>Winter is coming!</h3>  </body> </html>' | sudo tee /var/www/html/index.html
```

Аналогично для внутреннего сделаем:

```
1 echo '<!doctype html> <html> <body> <h1>SBT Networks 2019 Internal</h1> <h3>The night is dark and full of terrors.</h3>  </body> </html>' | sudo tee /var/www/html/index.html
```

Теперь про настройку VPN.

Эту часть брала [отсюда](#).

Переходим в Сеть VPC -> Маршруты.

Создаем новый маршрут (можно и через ui, но тут быстрее через Google Cloud Shell):

```
1 gcloud beta compute routes create route-cat --project=arcane-timer-262110 --network=
  mycatnet --priority=1000 --destination-range=199.36.153.4/30 --next-hop-
2 gateway=default-internet-gateway
```

Теперь перейдем в экземпляры ВМ и создадим новый инстанс (vpn gateway):

```
1 gcloud compute --project=arcane-timer-262110 instances create vpngate \
2   --zone=europe-west2-c --machine-type=n1-standard-1 \
3   --subnet=mycatnet1 --can-ip-forward --no-service-account \
4   --no-scopes --image-family=debian-9 --image-project=debian-cloud \
5   --image-project=debian-cloud --boot-disk-size=10GB \
6   --boot-disk-type=pd-standard --boot-disk-device-name=vpngate
```

Добавим теперь маршрут через VPN gateway:

```
1 gcloud compute routes create route-vpnka \
2   --network=mycatnet --priority=1000 \
3   --destination-range=199.36.153.4/30 --next-hop-instance=vpngate \
4   --next-hop-instance-zone=europe-west2-c
```

Переходим в Гибридное подключение -> VPN -> создать VPN-подключение.

Выбираем классическую VPN:

Затем заполняем данные про VPN-шлюз:

← Создание VPN-подключения

Виртуальные частные сети (VPN) позволяют подключаться к ресурсам Google Compute Engine в безопасном режиме. Они работают через туннели IPsec, которые создаются по протоколам IKEv1 или IKEv2. [Подробнее...](#)

VPN-шлюз Google Compute Engine ?

Название ?
Название нельзя будет изменить.

Описание (Необязательно)

Сеть ?

Регион ?

IP-адрес ?

При этом создаем IP-адрес (статический):

Резервирование статического IP-адреса

Название ?
Название нельзя будет изменить.

Описание (Необязательно)

[ОТМЕНА](#) [ЗАРЕЗЕРВИРОВАТЬ](#)

Заполняем VPN tunnel (тут 35.197.192.16 – внешний IP для инстанса vpngate):

Новый элемент

Название ?

Название нельзя будет изменить.

vpn-cat-tunnel-1

Описание (Необязательно)

IP-адрес удаленного узла ?

35.197.192.16

Версия IKE ?

IKEv2

Общий IKE-ключ

Ключ можно ввести самостоятельно или использовать сгенерированный автоматически

Создать и скопировать

⚠

Сохраните общий ключ в надежном месте. Его нельзя будет восстановить. [Подробнее...](#)

Настройки маршрутизации ?

Динамическая (BGP)

На основе маршрутов

На основе правил

Диапазоны IP-адресов удаленной сети ?

Чтобы ввести несколько диапазонов IP-адресов (в CIDR-нотации), нажимайте ВВОД после каждого из них.

10.0.0.0/9

Готово

Отмена

Трафик через VPN:

```

1 gcloud compute firewall-rules create allow-vpn-traffic --direction=INGRESS \
2   --priority=1000 --network=mycatnet \
3   --action=ALLOW --rules=tcp,udp,icmp \
4   --source-ranges=10.0.0.0/9

```

Так, при вызове из vpngate:

```

gorskaya_ev@vpngate:~$ ping 10.0.0.2
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
64 bytes from 10.0.0.2: icmp_seq=1 ttl=64 time=1.58 ms
64 bytes from 10.0.0.2: icmp_seq=2 ttl=64 time=0.290 ms
64 bytes from 10.0.0.2: icmp_seq=3 ttl=64 time=0.294 ms
64 bytes from 10.0.0.2: icmp_seq=4 ttl=64 time=0.253 ms
64 bytes from 10.0.0.2: icmp_seq=5 ttl=64 time=0.275 ms
64 bytes from 10.0.0.2: icmp_seq=6 ttl=64 time=0.309 ms
64 bytes from 10.0.0.2: icmp_seq=7 ttl=64 time=0.265 ms
^C
--- 10.0.0.2 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6116ms
rtt min/avg/max/mdev = 0.253/0.466/1.582/0.456 ms
gorskaya_ev@vpngate:~$ curl 10.0.0.2
<!doctype html> <html> <body> <h1>SBT Networks 2019 External</h1> <h3>Winter is coming!</h3>  </body> </html>
gorskaya_ev@vpngate:~$

```

2 Просмотр

Для перехода на внешний сервер можно использовать: <http://35.234.129.41/> (лучше не из этого файла переходить, а в адресную строку вбить).

Появится страница:

SBT Networks 2019 External

Winter is coming!

