

Знакомство с облачной инфраструктурой. Google Cloud Platform

План самостоятельной работы

- Создание учетной записи в GCP
- Создание в веб-интерфейсе инстансов VM и подключение к ним по SSH
- Рассмотрим варианты подключения к хостам через бастион-хост и VPN

Проверка домашнего задания

- Создайте новую ветку `cloud-bastion` в вашем репозитории `<yourname>_infra` для выполнения данного ДЗ
- Прием ДЗ будет производиться через *Pull Request* ветки с ДЗ к ветке `master` вашего репозитория
- После того, как будет получен approve пул реквеста, ветку с ДЗ **нужно** смерджить и закрыть PR

Создание учетной записи в Google Cloud Platform

Необходимо зарегистрироваться в GCP по ссылке:

- <https://cloud.google.com/free/>

Для регистрации рекомендуется использовать новую и отдельную учетную запись Google

Создание учетной записи в Google Cloud Platform

Google Cloud Platform Free Tier

Learn and build on GCP for free.

TRY IT FREE

Создание учетной записи в Google Cloud Platform



Попробуйте Cloud Platform бесплатно Google

Страна

Россия

Условия использования

Я хочу получать информацию о новых функциях, советы по повышению производительности, приглашения поделиться отзывом или поучаствовать в опросе, а также специальные предложения.

Да Нет

Я принимаю [Условия использования](#) и соглашаюсь с тем, что ими регулируется любое использование [сервисов и связанных с ними API](#). Я принимаю [Условия бесплатного пробного периода Google Cloud Platform](#).

Это обязательное поле.

Да Нет

[Принять и продолжить](#)

Создание учетной записи в Google Cloud Platform

Во время регистрации Google может запросить ввести данные платежной карты, это единственное платежное требование.

После окончания trial-периода Google **не будет** автоматически снимать средства с карты, **можно не волноваться**.

От предложений использовать карту после окончания trial-периода рекомендуется отказываться.

Создание учетной записи в Google Cloud Platform

Заполните поля, необходимые для регистрации



Попробуйте Cloud Platform бесплатно [Google](#)

Сведения о клиенте

Тип аккаунта
юридического лица

Наименование и адрес

Название компании
otus

Имя
otus otus

Первая строка адреса
Uchenicheskaya 12/3

Вторая строка адреса

Город
Moscow

Область Индекс
Москва 119000

Создание учетной записи в Google Cloud Platform

В конце успешной регистрации должно отобразиться окно приветствия



Добро пожаловать в Google Cloud Platform.

Пробный период активирован!

У вас есть кредит в размере 300 долл. США. Вы сможете пользоваться им в течение 12 месяцев. Напоминаем, что знакомство с нашим сервисом бесплатно. Мы не станем списывать с вашего счета средства, пока вы не решите перейти на полную версию.

[ИЗУЧИТЬ КОНСОЛЬ](#)

[ОК](#)

Основные элементы управления

The screenshot shows the Google Cloud Platform dashboard interface. At the top, there is a blue navigation bar with the Google Cloud Platform logo, a dropdown menu labeled "Выберите проект", a search bar, and a set of utility icons (mail, chat, help, notifications, user profile). Below the navigation bar, the main content area features several service cards. The first card is blue and titled "Запустите сервис Compute Engine". The second card is white and titled "Попробуйте Cloud Storage". The third card is white and titled "Изучите интерактивные руководства". There are also buttons for "Начать" and "Попробовать Cloud Storage".

Основные элементы управления:

- Начало работы:** Indicated by an orange arrow pointing to the hamburger menu icon in the top left corner.
- Выбор проекта с облачными сервисами:** Indicated by an orange arrow pointing to the "Выберите проект" dropdown menu.
- Основное меню облачных сервисов:** Indicated by an orange arrow pointing to the "Запустите сервис Compute Engine" card.
- Cloud shell, справочная информация и уведомления по учетной записи:** Indicated by an orange arrow pointing to the utility icons in the top right corner.

Создаем новый проект

Google Cloud Platform Выберите проект ▾

Начало работы

Выбор проекта с облачными сервисами

Запустите сервис Compute Engine

Создайте виртуальную машину Google Compute Engine и запустите в ней приложение "Список задач" на базе Node.js и MongoDB.

Попробовать Compute Engine

Попробуйте Cloud Storage

Cloud Storage – это мощный и удобный сервис хранения. Изучив наше руководство, вы узнаете, как создавать сегмент хранилища, загружать в него файлы и предоставлять доступ к ним по ссылке.

Попробовать Cloud Storage

Изучите интерактивные руководства

Из них вы узнаете, как создавать и развертывать простые приложения в Google Cloud Platform.

Начать

Создаем новый проект

Выбор области действия

Недавние Все


Название	Идентификатор
 Без организации	0




Создаем новый проект

Создание проекта

 Остаток проектов в рамках квоты: 11. [Подробнее...](#)

Название проекта 

Infra

Идентификатор проекта: infra-188718.  [Изменить](#)

Создать

Отмена

Работа с Google Compute Engine

В следующих заданиях мы будем работать с IaaS слоями Google Compute Platform:

- VPC сети (Virtual Private Network)
- GCE Metadata (для управления ключами доступа к серверам)
- GCE VM (для создания и управления инстансами виртуальных машин)

А также создадим пару ключей и привяжем ее к метаданным GCE (Google Compute Engine) для последующего получения доступа на виртуальные машины

Работа с Google Compute Engine

Из основного меню переходим в **Compute Engine (GCE)**,
дожидаемся активации

Compute Engine

Экземпляры VM

Экземпляры VM

Группы экземпляров

Шаблоны экземпляров

Диски

Снимки

Образы

Скидки за обязательства ...

Метаданные

Проверки состояния

Зоны

Операции

Квоты

Настройки

Идет активация Compute Engine. Это может занять несколько минут. [Документация по Compute Engine](#)

Compute Engine
Экземпляры VM

Сервис Compute Engine позволяет вам запускать свои собственные VM в инфраструктуре Google – от микромашин до более крупных систем, на которые можно устанавливать Debian, Windows и другие стандартные образы. Создайте экземпляр VM и импортируйте его через CloudEndure или запустите быструю настройку, чтобы развернуть типовое приложение.

[Создать](#) или [Перенести](#) или [Запустить мастер](#)

Работа с GCE: Метаданные

Для начала перейдем в раздел меню **Метадата**, выберем вкладку **SSH ключи** и нажмем **Добавить SSH-ключи**

The screenshot shows the Google Cloud Platform console interface. The top navigation bar includes the Google Cloud Platform logo, the 'Infra' dropdown menu, a search bar, and utility icons. The left sidebar contains a navigation menu with the following items: Compute Engine (selected), Экземпляры VM, Группы экземпляров, Шаблоны экземпляров, Диски, Снимки, Образы, Скидки за обязательства ..., **Метаданные** (highlighted with an orange arrow and the number 1), and Проверки состояния. The main content area is titled 'Метаданные' and features two tabs: 'Метаданные' and 'SSH-ключи' (selected with an orange arrow and the number 2). Below the tabs, there is a card titled 'Compute Engine SSH-ключи' containing explanatory text and a blue button labeled 'Добавить SSH-ключи' (highlighted with an orange arrow and the number 3).

Генерация пары ключей

На вашей пользовательской Linux/Unix системе сгенерировать пару ключей можно при помощи утилиты `ssh-keygen` (часть `ssh-agent`) (пример на следующем слайде)

После того как команда отработает, мы получаем пару из приватного и публичного ключей в домашнем каталоге текущего пользователя системы

- **Приватный ключ:**
 - `~/.ssh/appuser`
- **Публичный ключ:**
 - `~/.ssh/appuser.pub`

Генерация пары ключей

Пример вывода `ssh-keygen` (для пользователя `appuser`):

```
> ssh-keygen -t rsa -f ~/.ssh/appuser -C appuser -P ""
Generating public/private rsa key pair.
Your identification has been saved in /Users/Express42/.ssh/appuser.
Your public key has been saved in /Users/Express42/.ssh/appuser.pub.
The key fingerprint is:
SHA256:m0061ywMIY72dA2kpNEtKktb10jg2pvr2ajkRHoG6c appuser
The key's randomart image is:
+----[RSA 2048]-----+
|  .oo..                |
|  .+++                 |
|  .++o=                |
|  ..=+ +.=            |
|  .+===+oo S .        |
|  .o oB.oo B .        |
|   E.o  B =           |
|   ...= +             |
|  .o..= .             |
+-----[SHA256]-----+
```

Вносим в форму публичный ключ

Содержимое файла `~/ .ssh/appuser .pub` вносим в форму ввода ключа и сохраняем

Metadata

SSH Keys

appuser

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDF4Ebu0KmfD4zyu/37Pmws0jSN1VqtmOx1w/aBntIdC  
BZ/iMjqEME1FS3Te7MlkB4BiwpHyI+lmTXOLbXuMcpoHteFd3vKZdRSwqa+Qb49IYE1eJOBq1aJ9cDyoK  
d40VJgij36mRdX1YALREuFDSbHe4dcKRfwkcZwd/1Muabt+Dxpv0EjHHbpFMjzjXuyWdI1ry3Xb4t/zM0  
L2u7nrcmA6fmQtE9CR8eqDgDHgv2hzRmWj4+qoONkBpJBmgu3Jukxit8XBot2XzZYmIzSZBUSIGr0sy0H  
oy0+xe/mntyS1+n3wPBgvDZ5jp/N5t/aFwvquyra/vD9BgJPMUuk0M1Z appuser
```



+ Add item

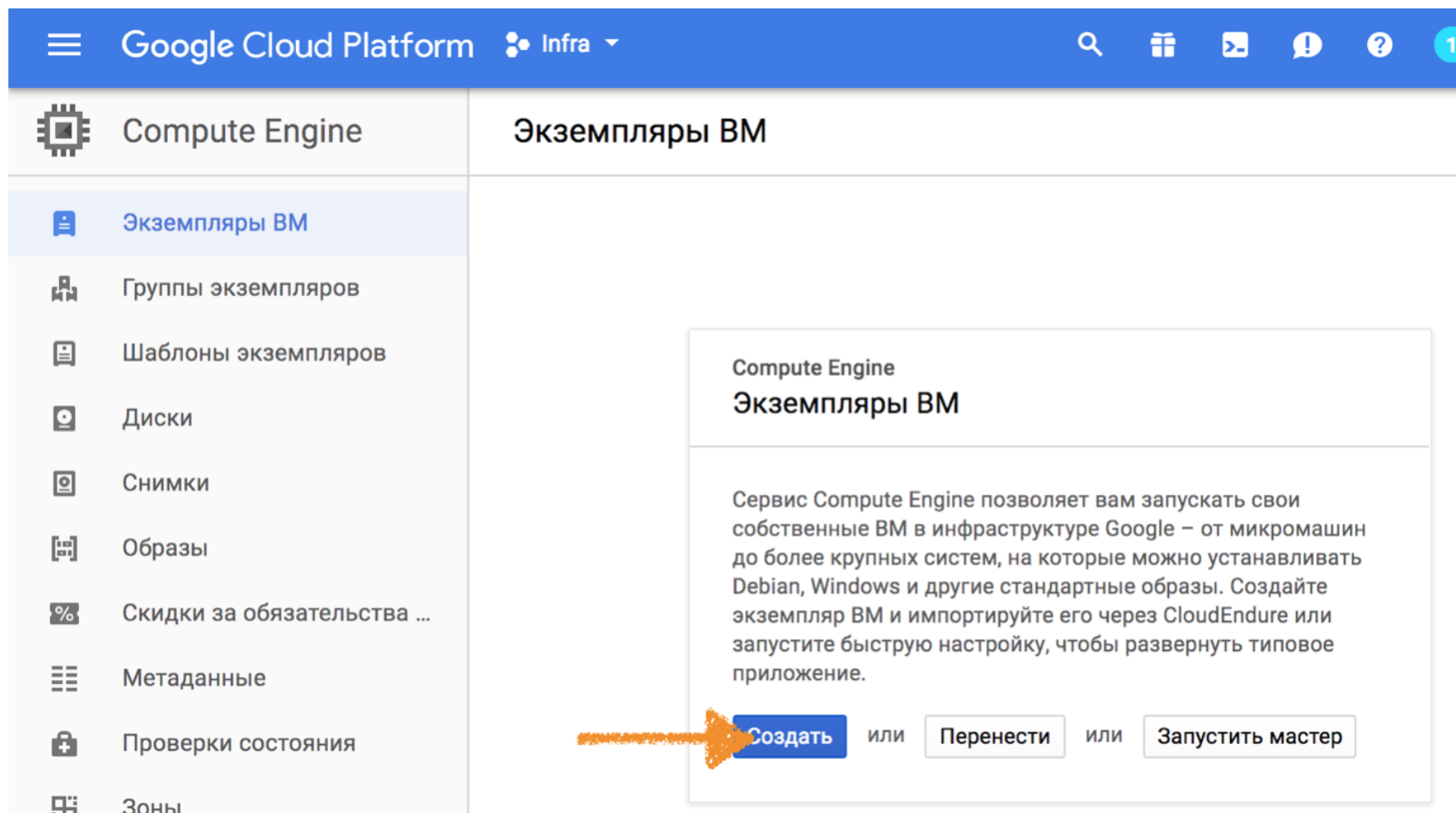
Save

Cancel

SSH-ключи в Метаданных проекта GCP

- Действуют на все виртуальные машины в проекте
- Могут быть переопределены при создании виртуальной машины
- Могут быть заблокированы при создании виртуальной машины - чтобы ни один из описанных в метадате проекта ключей не использовался

Создаем Экземпляр VM (инстанс)



The screenshot shows the Google Cloud Platform console interface. At the top, there is a blue header with the text 'Google Cloud Platform' and 'Infra'. Below the header, the left sidebar contains a navigation menu with items like 'Compute Engine', 'Экземпляры VM', 'Группы экземпляров', 'Шаблоны экземпляров', 'Диски', 'Снимки', 'Образы', 'Скидки за обязательства ...', 'Метаданные', 'Проверки состояния', and 'Зоны'. The main content area is titled 'Экземпляры VM' and contains a card with the following text:

Compute Engine
Экземпляры VM

Сервис Compute Engine позволяет вам запускать свои собственные VM в инфраструктуре Google – от микромашин до более крупных систем, на которые можно устанавливать Debian, Windows и другие стандартные образы. Создайте экземпляр VM и импортируйте его через CloudEndure или запустите быструю настройку, чтобы развернуть типовое приложение.

Below the text, there are three buttons: 'Создать' (highlighted with an orange arrow), 'Перенести', and 'Запустить мастер', separated by 'или'.

Создаем Экземпляр VM (инстанс)

Вбиваем имя хоста: **bastion**

Зона: **europa***

Тип машины: **микромашина**

Загрузочный диск: **Ubuntu 16.04**

← Создать экземпляр

Название ?

bastion

Зона ?

europa-west1-d

Тип машины

микромашина...

0,6 ГБ памяти

[Настроить](#)

Если вы [перейдете на платный аккаунт](#), то сможете создавать экземпляры с количеством ядер до 64.

Загрузочный диск ?



Новый стандартный постоянный диск объемом 10 ГБ
Образ
Ubuntu 16.04 LTS

[Изменить](#)

Создаем Экземпляр VM (инстанс)

Настройка параметров сети -> Сеть -> Сетевые интерфейсы

Оставляем сеть **default**

Внешний IP: **Создать адрес**

Название адреса: **bastion**

default сеть может отличаться от той, что на скриншоте, это нормально

Сетевые интерфейсы ?

Сетевой интерфейс

Сеть ?
default

Подсеть ?
default (10.132.0.0/20)

Основной внутренний IP-адрес ?
Назначается автоматически

✓ Показать псевдонимы диапазонов IP-адресов

Внешний IP-адрес ?
bastion (146.148.26.242)

IP-перенадресация ?
Выкл.

Готово Отмена

Создаем Экземпляр VM (инстанс)

Нажимаем **Создать** и дожидаемся готовности VM на панели Compute Engine

<input type="checkbox"/>	Название ^	Зона	Рекомендация	Внутренний IP-адрес	Внешний IP-адрес	Подключиться
<input checked="" type="checkbox"/>	bastion	us-central1-c		10.128.0.2	146.148.80.202	SSH ▾

Проверяем подключение по полученному внешнему адресу

Проверяем из локальной консоли подключение к созданной VM: `ssh -i ~/.ssh/appuser appuser@<внешний IP VM>`

```
$ ssh -i ~/.ssh/appuser appuser@<внешний IP VM>
The authenticity of host '<внешний IP VM> (<внешний IP VM>)' can't be established.
ECDSA key fingerprint is SHA256:Vp9dwnLwlyfLbWPpgR/bcFze0UIvuqCqhnG6uRjMzRo.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '<внешний IP VM>' (ECDSA) to the list of known hosts.
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.10.0-42-generic x86_64)
* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:       https://ubuntu.com/advantage
Get cloud support with Ubuntu Advantage Cloud Guest:
  http://www.ubuntu.com/business/services/cloud
0 packages can be updated.
0 updates are security updates.
appuser@bastion:~$ cat /etc/issue Ubuntu 16.04.3 LTS \n \l
```








Часть IaaS состоит из сетевого слоя, но это не значит, что управление им должно выполняться отдельно через раздел **VPC**

В нашем случае, при создании проектов автоматом было создано по одной приватной сети на каждый регион и шлюз для выхода в интернет









При создании VM мы также указали, что хотим завести статический внешний IP **bastion**, который также будет виден в разделе VPC


VPC: Приватные сети

Из главного меню, откройте раздел VPC:

 Сеть VPC	Сети VPC + СОЗДАТЬ СЕТЬ VPC ↻ ОБНОВИТЬ						
 Сети VPC	Название ^	Регион	Подсети	Режим	Диапазоны IP-адресов	Шлюзы	Правила брандмауэра
 Внешние IP-адреса	default		11	Автоматический ▾			4
 Правила брандмауэра		us-central1	default		10.128.0.0/20	10.128.0.1	
 Маршруты		europa-west1	default		10.132.0.0/20	10.132.0.1	
 Точки обмена данными V...		us-west1	default		10.138.0.0/20	10.138.0.1	
 Общая сеть VPC		asia-east1	default		10.140.0.0/20	10.140.0.1	
		us-east1	default		10.142.0.0/20	10.142.0.1	
		asia-northeast1	default		10.146.0.0/20	10.146.0.1	
		asia-southeast1	default		10.148.0.0/20	10.148.0.1	
		us-east4	default		10.150.0.0/20	10.150.0.1	
		australia-southeast1	default		10.152.0.0/20	10.152.0.1	
		europa-west2	default		10.154.0.0/20	10.154.0.1	
		europa-west3	default		10.156.0.0/20	10.156.0.1	

VPC: Публичные адреса

 Сеть VPC	Внешние IP-адреса    ПОКАЗАТЬ ИНФОРМАЦИЮ					
 Сети VPC						
 Внешние IP-адреса						
 Правила брандмауэра						
 Маршруты						

<input type="checkbox"/>	Название	Внешний адрес	Регион	Тип ▼	Версия	Используется
<input type="checkbox"/>						
<input type="checkbox"/>	bastion	146.148.80.202	us-central1	Статический ▼	IPv4	Экземпляр bastion Зона с

VPC

Примеры управления сетями и разделение топологий будут описаны в будущих лекциях, с использованием инструментов, работающих через API

Создаем вторую VM без внешней сети

По аналогии с предыдущими шагами по созданию VM, инициировать создание второй машины с именем **someinternalhost**

Среди отличий в создании, в разделе управления сетями, **необходимо убрать создание публичного адреса** (см. скриншот)

Сетевой интерфейс

Сеть ?
default

Подсеть ?
default (10.128.0.0/20)

Основной внутренний IP-адрес ?
Назначается автоматически

Показать псевдонимы диапазонов IP-адресов








Внешний IP-адрес ?
Нет

IP-перееадресация ?
Выкл.

Готово Отмена

Проверяем результат

Compute Engine

Экземпляры VM        [ПОКАЗАТЬ ИНФОРМАЦИОННУЮ ПАНЕЛЬ](#)

Экземпляры VM

Группы экземпляров

Шаблоны экземпляров

Диски

Снимки

Образы

Введите фильтр

Столбцы

<input type="checkbox"/> Название ^	Зона	Рекомендация	Внутренний IP-адрес	Внешний IP-адрес	Подключиться
<input checked="" type="checkbox"/> bastion	us-central1-c		10.128.0.2	146.148.80.202	SSH ▾ ⋮
<input checked="" type="checkbox"/> someinternalhost	europa-west1-d		10.132.0.2	Не задан	SSH ▾ ⋮

Рассмотрим текущее состояние хостов

Для верности эксперимента, пробуем зайти по SSH на `bastionhost`, а с него по внутреннему адресу на `someinternalhost` (используйте ваши адреса)

```
$ ssh -i ~/.ssh/appuser appuser@146.148.80.202
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.10.0-32-generic x86_64)
...
0 packages can be updated.
0 updates are security updates.
Last login: Tue Aug 29 06:32:23 2017 from 79.164.31.28
To run a command as administrator (user "root"), use "sudo <command>". See "man
sudo_root" for details.
appuser@bastion:~$ ssh 10.132.0.2
Permission denied (publickey).
appuser@bastion:~$
```

Результат неудовлетворителен 😞

Используем Bastion host для прямого подключения к инстансам внутренней сети

Настроим SSH Forwarding на вашей локальной машине:

```
$ ssh-add -L  
The agent has no identities.
```

Добавим приватный ключ в ssh агент авторизации:

```
$ ssh-add ~/.ssh/appuser  
Identity added: /Users/otus/.ssh/appuser (/Users/otus/.ssh/appuser)
```

Используем Bastion host для сквозного подключения

Пробуем подключаться вновь, добавив в параметры подключения ключик **-A**, чтобы явно включить SSH Agent Forwarding

```
$ ssh -i ~/.ssh/appuser -A appuser@146.148.80.202
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.10.0-32-generic x86_64)
```

```
appuser@bastion:~$ ssh 10.132.0.2
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.10.0-32-generic x86_64)
...
Last login: Tue Aug 29 06:32:27 2017 from 10.128.0.2
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
```

Используем Bastion host для сквозного подключения

Убедимся, что попали на нужный хост:

```
appuser@someinternalhost:~$ hostname  
someinternalhost
```

```
appuser@someinternalhost:~$ ip a show ens4  
2: ens4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1460 qdisc pfifo_fast state UP group  
default qlen 1000  
    link/ether 42:01:0a:84:00:02 brd ff:ff:ff:ff:ff:ff  
    inet 10.132.0.2/32 brd 10.132.0.2 scope global ens4  
    valid_lft forever preferred_lft forever  
    inet6 fe80::4001:aff:fe84:2/64 scope link  
    valid_lft forever preferred_lft forever
```

Успех, но не очень удобно 😊

Проверим отсутствие каких-либо приватных ключей на bastion машине:

```
appuser@bastion:~$ ls -la ~/.ssh/  
total 16  
drwx----- 2 appuser appuser 4096 Aug 29 06:07 .  
drwxr-xr-x 4 appuser appuser 4096 Aug 29 06:07 ..  
-rw----- 1 appuser appuser 397 Aug 29 05:50 authorized_keys  
-rw-r--r-- 1 appuser appuser 222 Aug 29 06:03 known_hosts
```

Самостоятельное задание

Исследовать способ подключения к `someinternalhost` в одну команду из вашего рабочего устройства, проверить работоспособность найденного решения и внести его в **README.md** в вашем репозитории

Дополнительное задание:

Предложить вариант решения для подключения из консоли при помощи команды вида `ssh someinternalhost` из локальной консоли рабочего устройства, чтобы подключение выполнялось по алиасу `someinternalhost` и внести его в **README.md** в вашем репозитории

Создаем VPN-сервер для серверов GCP

Не удаляя предыдущие серверы, создадим схему с VPN-сервером [Pritunl](#), после сгенерируем конфигурацию VPN-клиента и подключимся к VPN-сети с последующим доступом в частную сеть облака

Создаем VPN-сервер для серверов GCP

Перед установкой перейдем в настройки **bastion** VM через Панель управления и разрешим в Брандмауэре **HTTP/HTTPS-трафик**

Брандмауэры

- Разрешить трафик HTTP
- Разрешить трафик HTTPS

Создаем VPN-сервер для серверов GCP

На хосте `bastion` выполняем команды [Ссылка на gist](#)

```
$ cat <<EOF> setupvpn.sh
#!/bin/bash
echo "deb http://repo.mongodb.org/apt/ubuntu xenial/mongodb-org/3.4 multiverse" > /etc/
apt/sources.list.d/mongodb-org-3.4.list
echo "deb http://repo.pritunl.com/stable/apt xenial main" > /etc/apt/sources.list.d/
pritunl.list
apt-key adv --keyserver hkp://keyserver.ubuntu.com --recv
0C49F3730359A14518585931BC711F9BA15703C6
apt-key adv --keyserver hkp://keyserver.ubuntu.com --recv
7568D9BB55FF9E5287D586017AE645C0CF8E292A
apt-get --assume-yes update
apt-get --assume-yes upgrade
apt-get --assume-yes install pritunl mongodb-org
systemctl start pritunl mongod
systemctl enable pritunl mongod
EOF
```

Создаем VPN-сервер для серверов GCP

Затем выполняем:

```
$ sudo bash setupvpn.sh
```

В результате:

- В текущей директории будет создан файл `setupvpn.sh`, описывающий установку VPN-сервера
- Будет установлена `mongodb` и VPN-сервер `pritunl`

Создаем VPN-сервер для серверов GCP

- Открываем в браузере ссылку: `https://<адрес bastion VM>/setup`
- Ошибку SSL пропускаем и доверяем этому сайту
- Следуем инструкциям на экране (запрашиваемые команды запускать через `sudo`)

Создаем VPN-сервер для серверов GCP








В конце установки авторизуемся, используя логин/пароль **pritunl/pritunl**

Далее добавляем в веб интерфейсе:

- Организацию
- Пользователя **test** с PIN **6214157507237678334670591556762**
- Сервер (затем привязываем его к организации и запускаем)

Подробнее: <https://docs.pritunl.com/v1/docs/connecting>

Создаем VPN-сервер для серверов GCP

Server	test
 Status	Online
 Uptime	0d 0h 4m 52s
 Users	0/1 users online
 Devices	0 devices online
 Network	192.168.229.0/24
 Port	12567/udp
 Multiple Devices	Disabled



Запомните порт,
на котором поднялся сервер

Создаем VPN-сервер для серверов GCP

Далее:

- Создадим правило для открытия порта VPN, в данном случае `udp:10855` (порт указывается при создании сервера)
- Добавим в инстансе `bastion` в **Теги сети** наше новое правило

Создаем VPN-сервер для серверов GCP

Сеть VPC

Сети VPC

Внешние IP-адреса

Правила брандмауэра

Маршруты

Точки обмена данными V...

Общая сеть VPC

Правила брандмауэра

[+ СОЗДАТЬ ПРАВИЛО БРАНДМАУЭРА](#) [ОБНОВИТЬ](#)

С помощью правил брандмауэра можно управлять входящим и исходящим трафиком для экземпляра. По умолчанию блокируется весь входящий трафик из-за пределов вашей сети. [Подробнее...](#)

Примечание. Управление брандмауэрами App Engine можно [здесь](#).

Входящий трафик Исходящий трафик

<input type="checkbox"/>	Название	Целевые экземпляры	Фильтры – сети-источники	Протоколы/порты	Действие	Приоритет
<input type="checkbox"/>	default-allow-http	http-server	Диапазоны IP-адресов: 0.0.0.0/0	tcp:80	Разрешить	1000
<input type="checkbox"/>	default-allow-https	https-server	Диапазоны IP-адресов: 0.0.0.0/0	tcp:443	Разрешить	1000
<input type="checkbox"/>	vpn-10855	vpn-10855	Диапазоны IP-адресов: 0.0.0.0/0	udp:10855	Разрешить	1000

Создаем VPN-сервер для серверов GCP

The screenshot displays the Pritunl web interface. At the top, there is a navigation bar with the Pritunl logo and menu items: Dashboard, Users, Servers, Upgrade to Enterprise!, Logs, Settings, and Logout. Below the navigation bar, the main heading is 'Users and Organizations'. To the right of this heading are four buttons: 'Add Organization', 'Add User', 'Bulk Add Users', and 'Delete Selected'. The main content area shows an organization named 'test' with a green 'Organization' label. To the right of the organization name, there is a '1 users' indicator, a search bar labeled 'Search for user', and a 'Delete Organization' button. Below this, a table lists the user 'test' with a status of 'Offline'. An orange arrow points to the download icon in the user's action menu.

Таким образом, мы установили и сконфигурировали OpenVPN-сервер Pritunl

Теперь надо скачать конфигурационный файл для подключения (см. стрелку на скриншоте)

Проверяем подключение к VPN

- Добавьте полученный конфигурационный файл `*.ovpn` в клиент OpenVPN на вашем компьютере
- Проверьте подключение к VPN-серверу
- Проверьте возможность подключения к `someinternalhost` с вашего компьютера после подключения к VPN:

```
$ ssh -i ~/.ssh/appuser appuser@<внутренний IP someinternalhost>
```

Дополнительное задание

Сейчас веб-интерфейс VPN-сервера Pritunl работает с самоподписанным сертификатом. И браузер постоянно ругается на это.

С помощью сервисов sslip.io/xip.io и [Let's Encrypt](https://letsencrypt.org/) реализуйте использование валидного сертификата для панели управления VPN-сервера

Задание

1. Выполните задание про подключение через бастион хост.
2. Добавьте в ваш репозиторий Infra (ветка `cloud-bastion`):
 - файл `setupvpn.sh`
 - конфигурационный файл для подключения к VPN (переименуйте `*.ovpn` в `cloud-bastion.ovpn`)
3. Опишите в `README.md` и получившуюся конфигурацию и данные для подключения в **следующем формате** (важно для проверки!):

```
bastion_IP = 35.198.167.169
someinternalhost_IP = 10.156.0.3
```

4. Добавьте "Labels" `cloud-bastion` к вашему Pull Request

Задание

► После успешного выполнения автоматической проверки в TravisCI можете удалить **оба** инстанса (`bastion` и `someinternalhost`) и **постоянный IP** адрес.