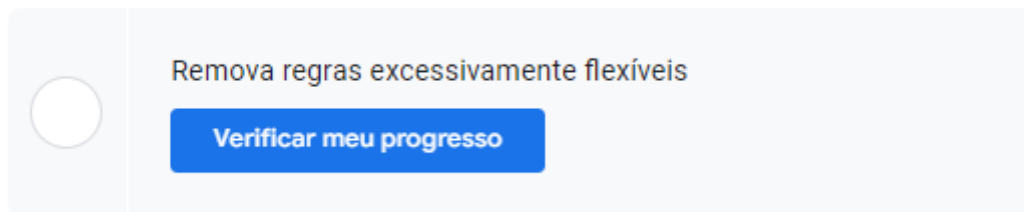
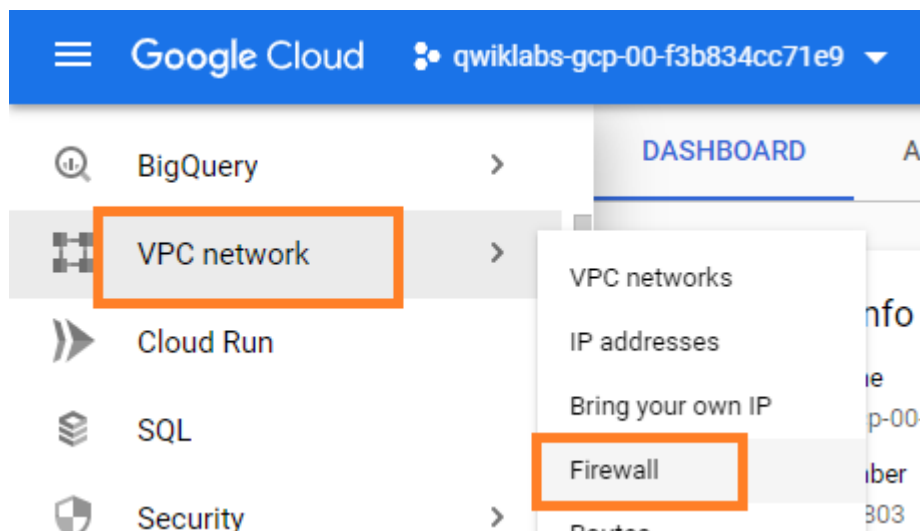


Resolução do desafio – Laboratório 2 (<https://www.cloudskillsboost.google/quests/128>)

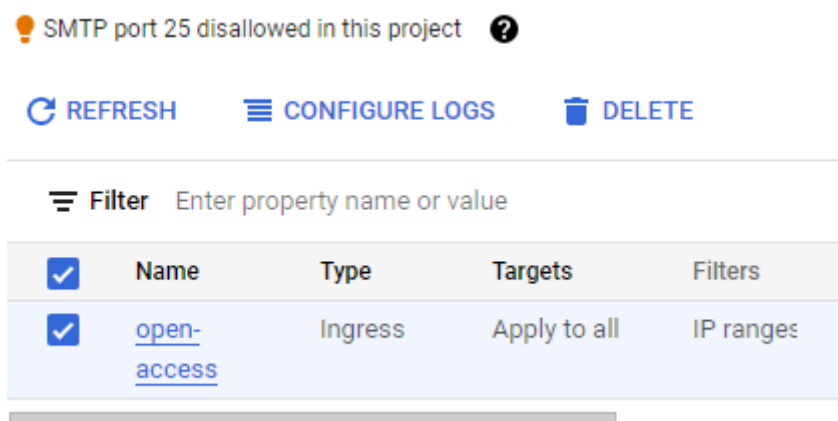


Acessar o console e ir ao painel de serviços do lado esquerdo da tela:

Procurar por “VPC network” e clicar em “Firewall”.

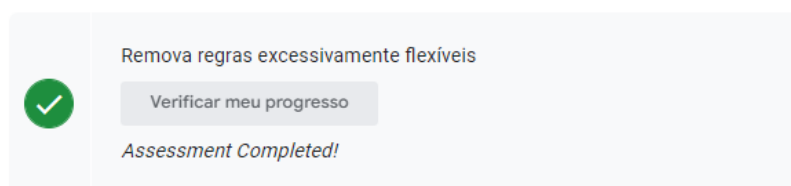


Procure pela regra abaixo, selecione e depois clique em “Delete”.



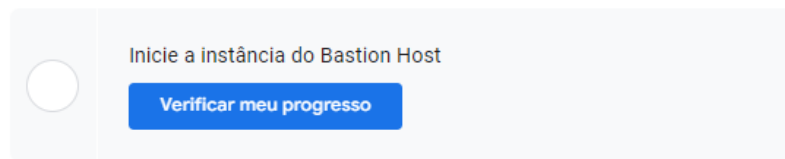
Após remover a regra, valide a primeira parte do laboratório.

1. Verifique as regras de firewall. Remova regras excessivamente flexíveis.

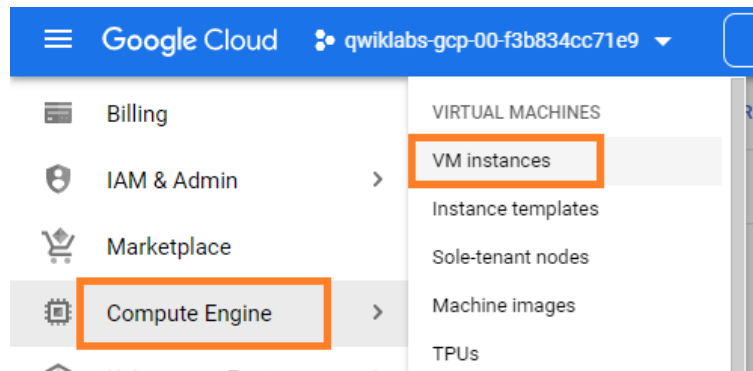


Segunda parte do laboratório.

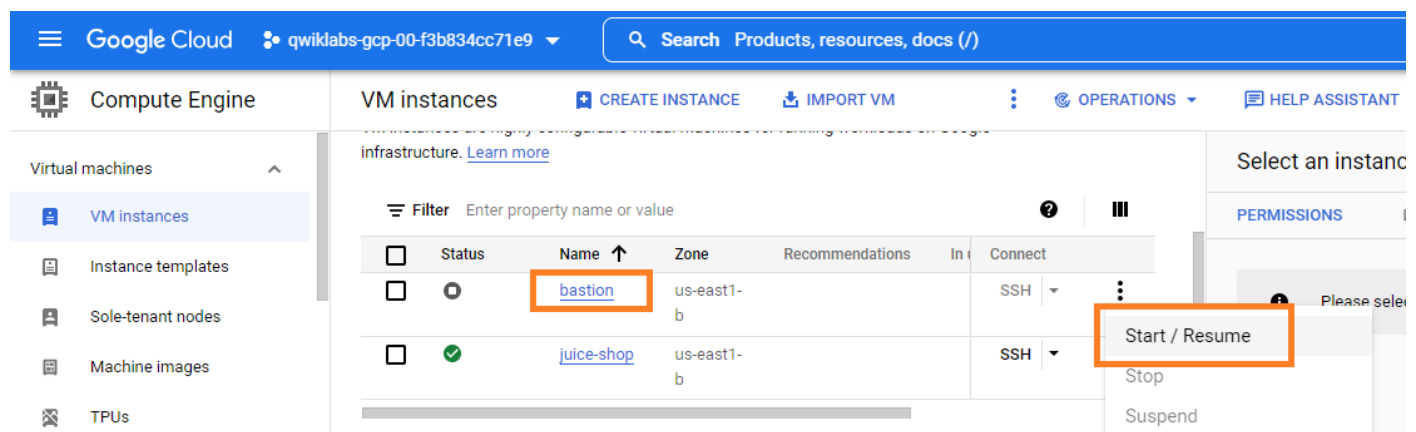
2. Acesse o Compute Engine no Console do Cloud e identifique o Bastion Host. A instância não deve estar em execução. Inicie a instância.



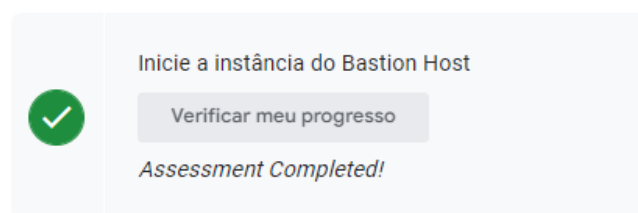
No menu lateral, procure por “Compute engine” e depois clique em “VM instances”



Encontre a instância chamada “Bastion” e clique em “Start” para colocá-la para executar.



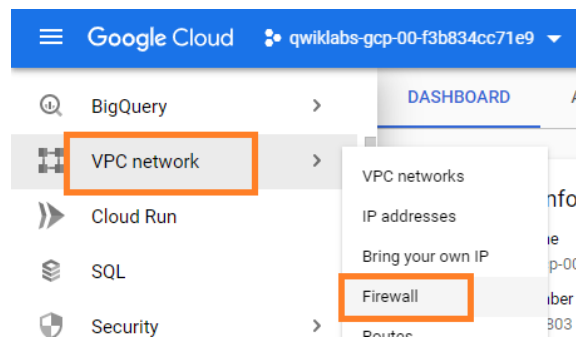
Após isso, aguarde o processo e valide a segunda parte.



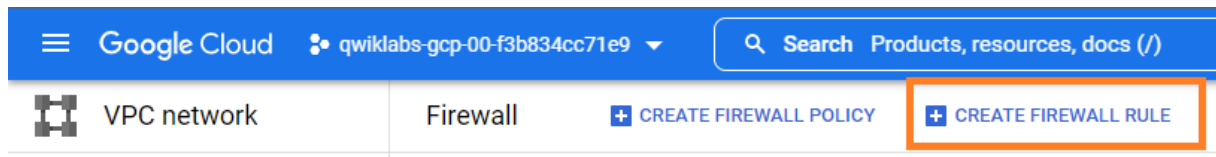
Terceira parte:

3. O Bastion Host é a única máquina autorizada a receber tráfego SSH externo. Crie uma regra de firewall que permita o tráfego [SSH \(TCP/22\) do serviço IAP](#). Ela precisa ser ativada na instância do Bastion Host com uma tag de rede de `grant-ssh-iap-ingress-q1-528`.

Volte no menu da esquerda em “VPC network” e depois clique em “Firewall”.



Depois clique em “Create firewall rule”



Preencha um nome a sua escolha e depois selecione clique no campo “Network” e selecione a rede que já está na listagem.

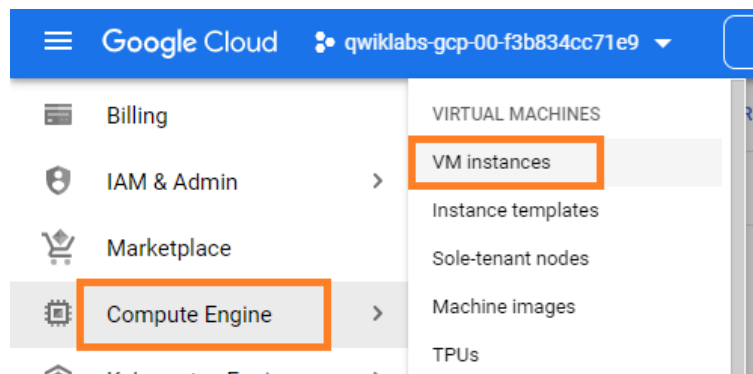
Ainda na mesma tela, desça um pouco e procure por “Target tags”. Coloque o nome indicado no seu laboratório.

No campo “Source IPv4 ranges” informe o valor **35.235.240.0/20**.

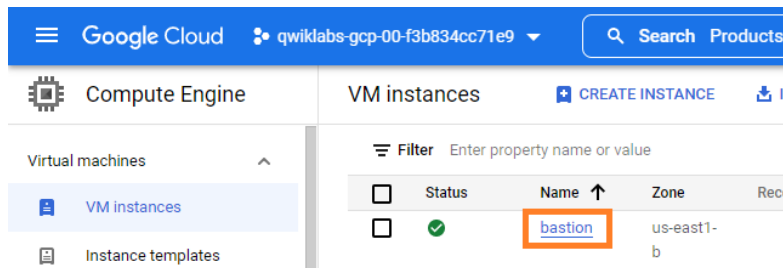
Marque a caixa do TCP e indique a porta **22**

Depois clique em “Create” ao final da página.

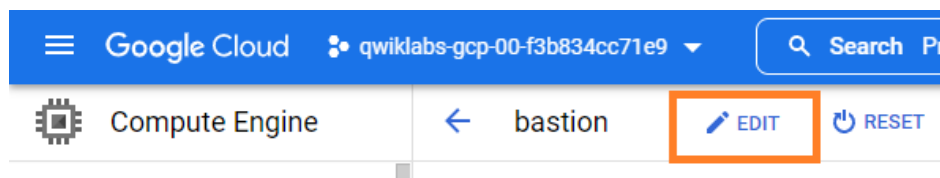
Volte no menu da esquerda em “Compute engine” e depois clique em “VM instances”



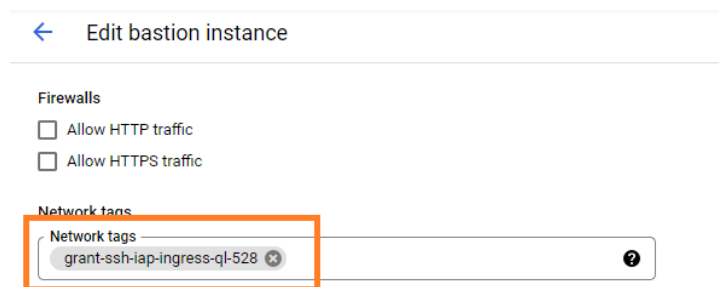
Clique sobre o nome da instância “bastion”



Depois clique sobre o botão “Edit” na faixa azul acima da tela.

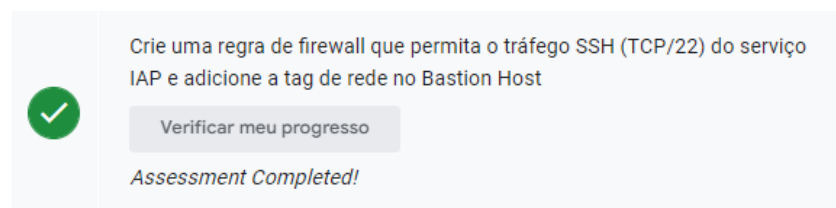


Desça na tela até encontrar a categoria “Network” e no campo “Network tags” informe o mesmo nome que seu laboratório indicou, o qual foi usado na etapa anterior.



Depois clique em “Save” na parte inferior da tela.

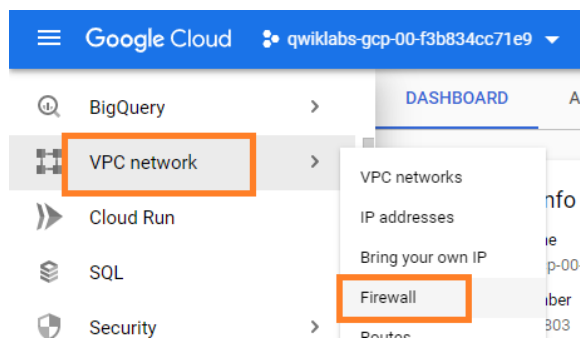
Aguarde o processo e depois valide a terceira parte do laboratório.



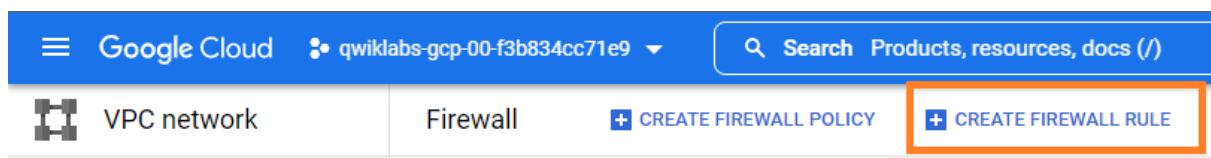
Quarta parte

4. O servidor de `juice-shop` direciona o tráfego HTTP. Crie uma regra de firewall que permita o tráfego HTTP (TCP/80) para qualquer endereço. Ela precisa ser ativada na instância de `juice-shop` usando uma tag de rede de `grant-http-ingress-ql-417`

Volte no menu da esquerda em “VPC network” e depois clique em “Firewall”.



Depois clique em “Create firewall rule”



Preencha um nome a sua escolha e depois selecione clique no campo “Network” e selecione a rede que já está na listagem.

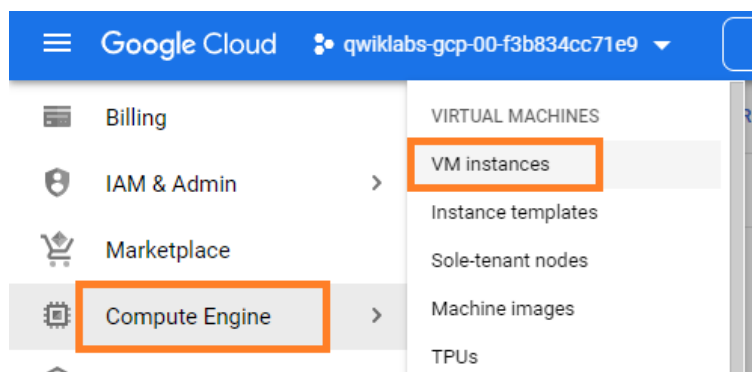
Ainda na mesma tela, desça um pouco e procure por “Target tags”. Coloque o nome indicado no seu laboratório.

No campo “Source IPv4 ranges” informe o valor **0.0.0.0/0**.

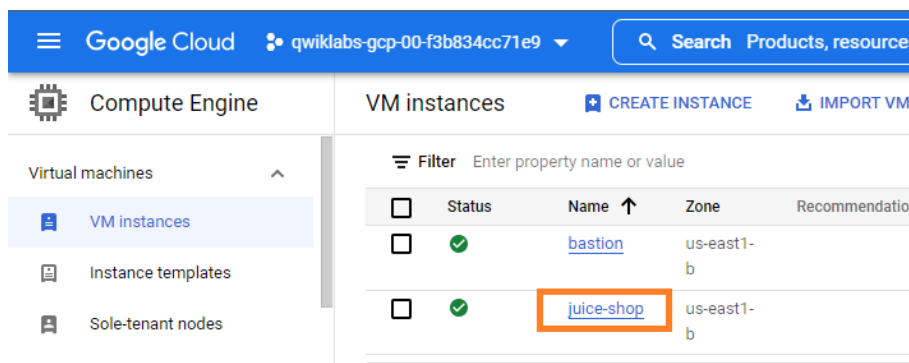
Marque a caixa do TCP e indique a porta **80**

Clique em “Create” ao final da página.

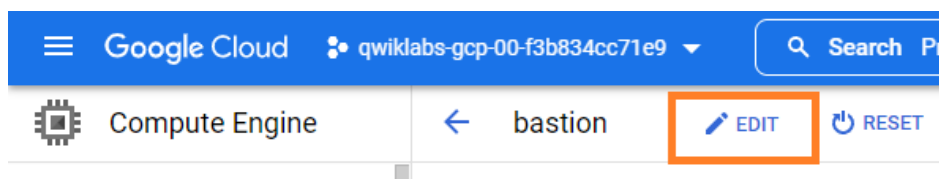
Volte no menu da esquerda em “Compute engine” e depois clique em “VM instances”



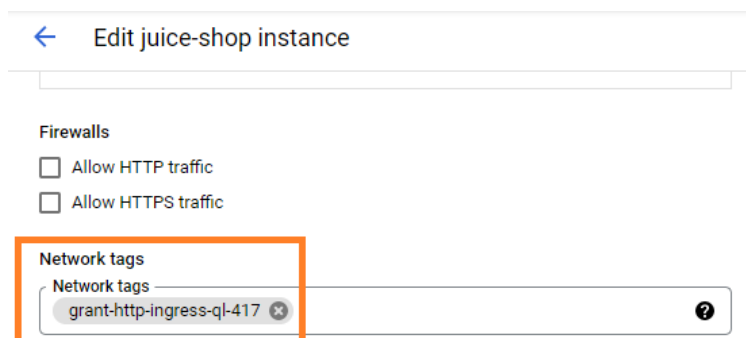
Clique sobre o nome da instância “juice-shop”



Depois clique sobre o botão “Edit” na faixa azul acima da tela.

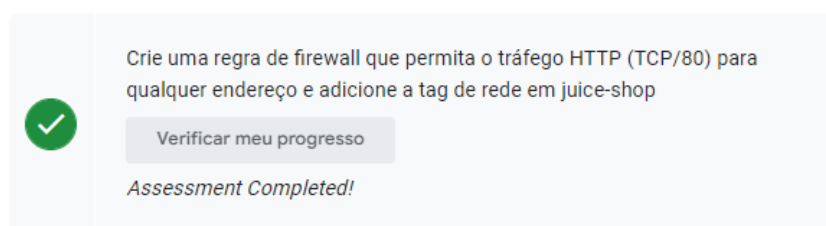


Desça na tela até encontrar a categoria “Network” e no campo “Network tags” informe o mesmo nome que seu laboratório indicou, o qual foi usado na etapa anterior.



Clique em “Save” ao final da página.

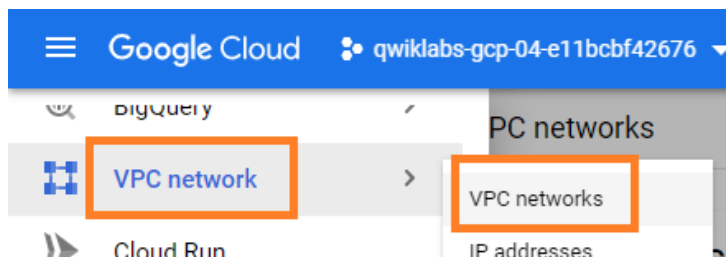
Volte para validar a quarta parte



Quinta parte

5. Você precisa se conectar a `juice-shop` no Bastion Host usando SSH. Crie uma regra de firewall que permita o tráfego SSH (TCP/22) do endereço de rede `acme-mgmt-subnet`. Ela precisa ser ativada na instância de `juice-shop` usando uma tag de rede de `grant-ssh-internal-ingress-ql-767`.

Volte no menu da esquerda em “VPC network” e depois clique em “VPC networks”.



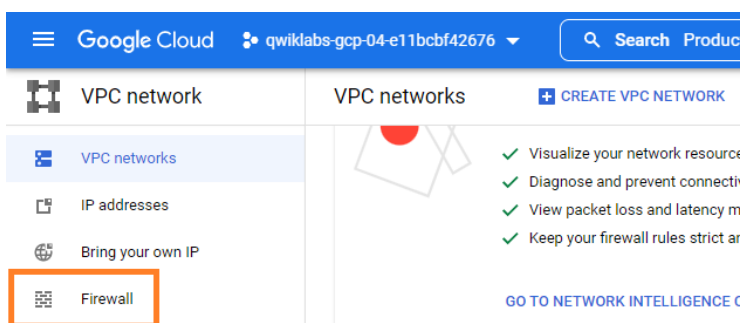
Procure pela rede que foi indicada no seu laboratório.

Copie o valor do IP indicado pela seta. Guarde esse valor anotado em algum lugar.

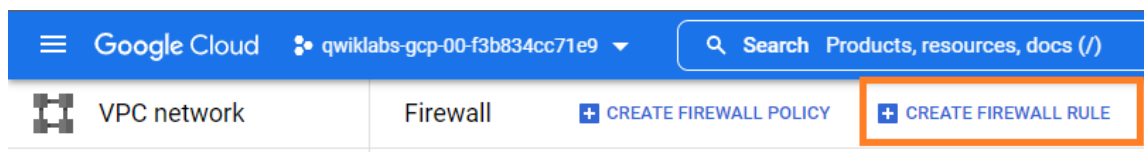
A screenshot of the Google Cloud console showing the 'VPC networks' page. The left-hand navigation menu is open, with 'VPC networks' selected. The main content area displays a table of VPC networks. The table has columns: Name, Region, Subnets, MTU, Mode, and Internal IP ranges. The first row is 'acme-vpc' with 2 subnets. The second row is 'acme-mgmt-subnet' with an internal IP range of 192.168.10.0/24. An orange box highlights the 'acme-mgmt-subnet' row. An orange arrow points from the '192.168.10.0/24' IP range to the right.

Name	Region	Subnets	MTU	Mode	Internal IP ranges
acme-vpc		2	1460	Custom	None
acme-mgmt-subnet	us-east1	acme-mgmt-subnet			192.168.10.0/24

Volte no menu da esquerda e clique em “Firewall”.



Depois clique em “Create firewall rule”



Preencha um nome a sua escolha e depois selecione clique no campo “Network” e selecione a rede que já está na listagem.

← Create a firewall rule

Firewall rules control incoming or outgoing traffic to an instance. By default, incoming traffic from outside your network is blocked. [Learn more](#)

Name *
firewall3
Lowercase letters, numbers, hyphens allowed

Description

Logs
Turning on firewall logs can generate a large number of logs which can increase costs in Cloud Logging. [Learn more](#)
☐ On
☒ Off

Network *
acme-vpc

Ainda na mesma tela, desça um pouco e procure por “Target tags”. Coloque o nome indicado no seu laboratório. No campo “Source IPv4 ranges” informe o valor do IP de acme-mgmt-subnet que foi copiado na etapa anterior. Marque a caixa do TCP e indique a porta **22**

← Create a firewall rule

Targets
Specified target tags

Target tags *
grant-ssh-internal-ingress-ql-767

Source filter
IPv4 ranges

Source IPv4 ranges *
192.168.10.0/24 for example, 0.0.0.0/0, 192.168.2.0/24

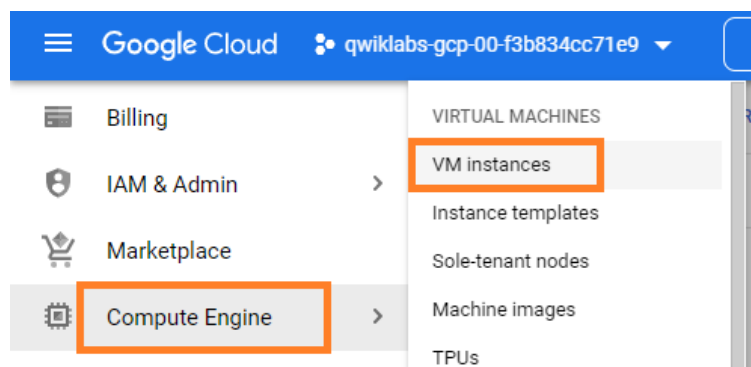
Second source filter
None

Protocols and ports
☐ Allow all
☒ Specified protocols and ports

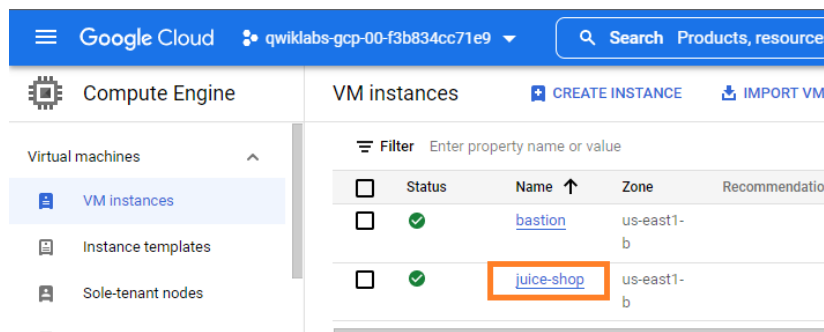
☒ TCP
Ports
22

Clique em “Create” ao final da tela.

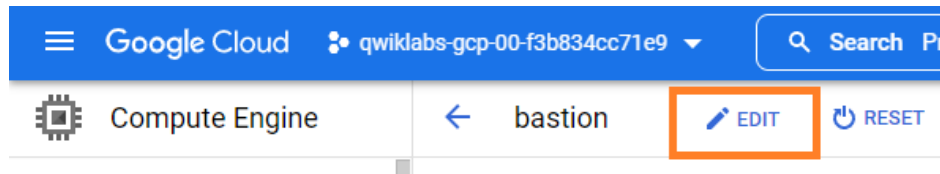
Volte no menu da esquerda em “Compute engine” e depois clique em “VM instances”



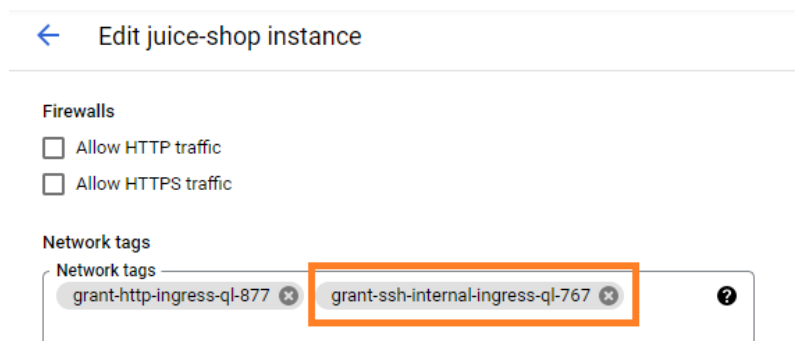
Clique sobre o nome da instância “juice-shop”



Depois clique sobre o botão “Edit” na faixa azul acima da tela.

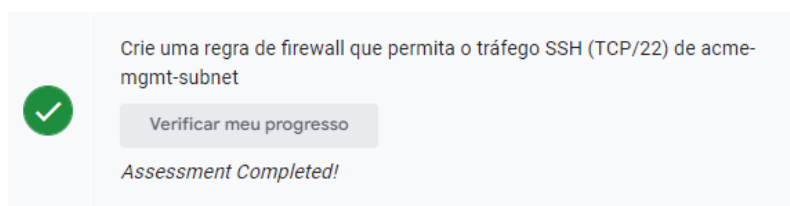


Desça na tela até encontrar a categoria “Network” e no campo “Network tags” adicione o mesmo nome que seu laboratório indicou, o qual foi usado na etapa anterior.



Clique em “Save” ao final da página.

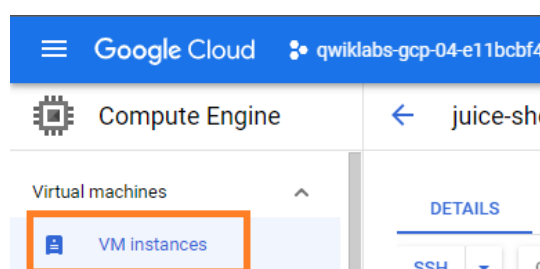
Volte para validar a quinta parte do laboratório.



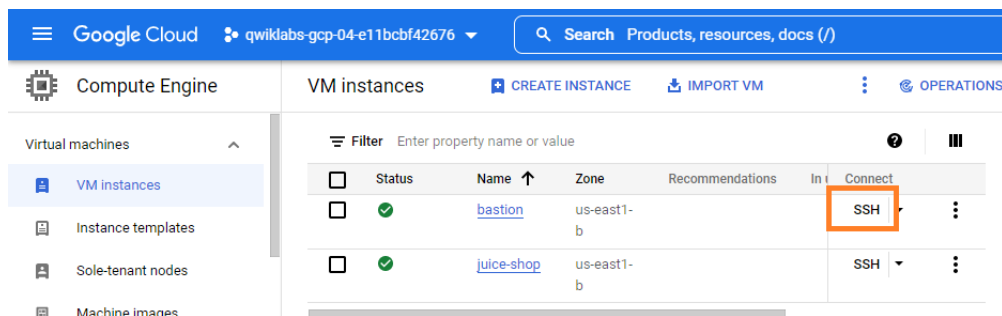
Sexta parte

6. Na página de instâncias do Compute Engine, clique no botão SSH para o Bastion Host. Quando conectado, estabeleça uma conexão SSH com `juice-shop`.

Volte para listar todas as instâncias de VM clicando em “VM instances” no menu da lateral esquerda.



Na linha da instância “bastion” clique sobre o botão “SSH”



Uma nova tela irá se abrir.

Aguarde o carregamento dessa tela finalizar.

Após carregar digite o seguinte comando e depois aperte ENTER para executar.

```
gcloud compute ssh juice-shop --internal-ip
```

Pressione “y” para confirmar e ENTER para continuar.

```
SSH-in-browser

Linux bastion 5.10.0-18-cloud-amd64 #1 SMP Debian 5.10.140-1 (2022-09-02) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Creating directory '/home/student-01-98b2b934d42d'.
student-01-98b2b934d42d@bastion:~$ gcloud compute ssh juice-shop --internal-ip
WARNING: The private SSH key file for gcloud does not exist.
WARNING: The public SSH key file for gcloud does not exist.
WARNING: You do not have an SSH key for gcloud.
WARNING: SSH keygen will be executed to generate a key.
This tool needs to create the directory [/home/student-01-98b2b934d42d/.ssh] before
being able to generate SSH keys.

Do you want to continue (Y/n)? y
```

Quando aparecer a seguinte mensagem

```
Do you want to continue (Y/n)? y

Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
```

Não escreva nada e só aperte ENTER duas vezes para continuar.

A seguinte mensagem irá aparecer

```
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/student-01-98b2b934d42d/.ssh/google_compute_engine
Your public key has been saved in /home/student-01-98b2b934d42d/.ssh/google_compute_engine.pub
The key fingerprint is:
SHA256:CD7gT4IY40NsRMgR8tY4FyJEBddqMVCzayk42DR6As student-01-98b2b934d42d@bastion
The key's randomart image is:
+---[RSA 3072]-----+
|O*=+..+|
|+=*B++ =|
|o=B=O. +|
|E O..o.|
|oo= . S|
|. = .|
|. .|
| .|
| |
+---[SHA256]-----+
Did you mean zone [us-east1-b] for instance: [juice-shop] (Y/n)?
```

Digite “y” e pressione ENTER.

Volte no laboratório e valide a última etapa



Estabeleça uma conexão SSH com o Bastion Host pelo IAP e com juice-shop pelo Bastion Host

Verificar meu progresso

Assessment Completed!