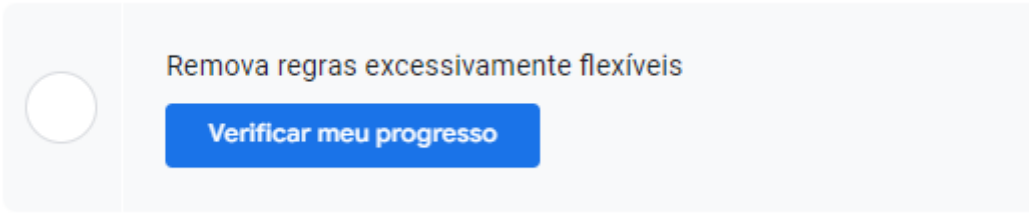
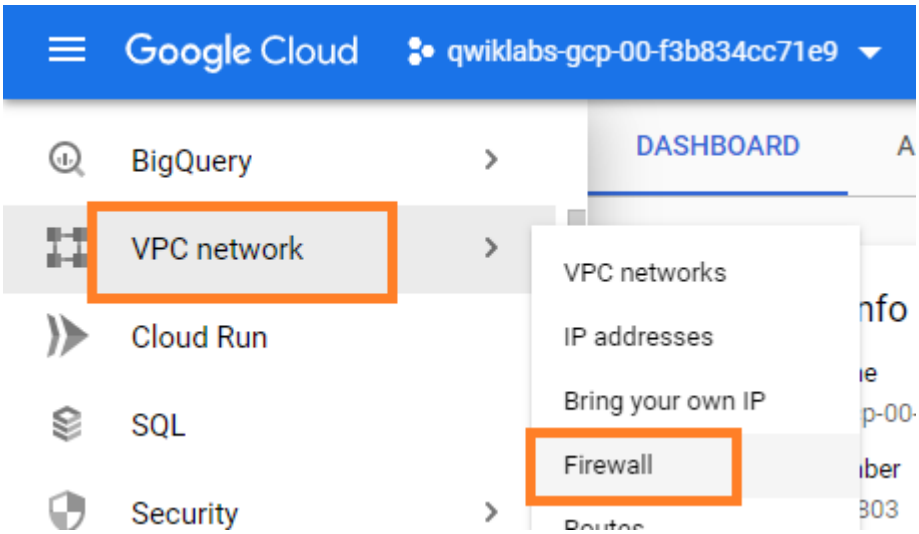
Resolução do desafio – Laboratório 2 (https://www.cloudskillsboost.google/quests/128)

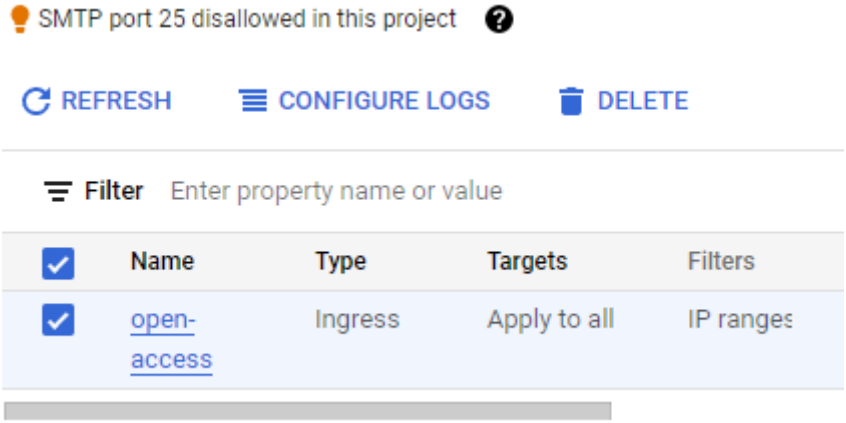


Acessar o console e ir ao painel de serviços do lado esquerdo da tela:

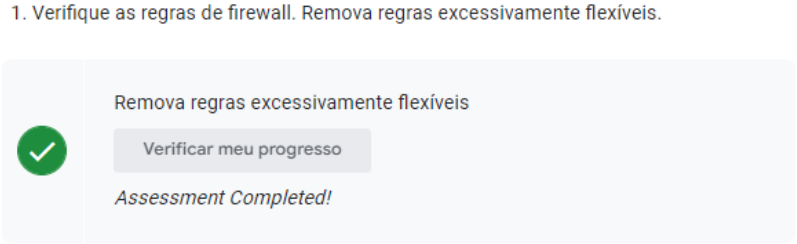
Procurar por “VPC network” e clicar em “Firewall”.



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

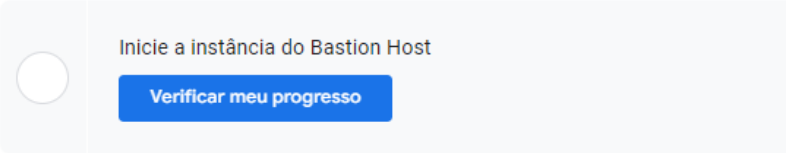


Após remover a regra, valide a primeira parte do laboratório.

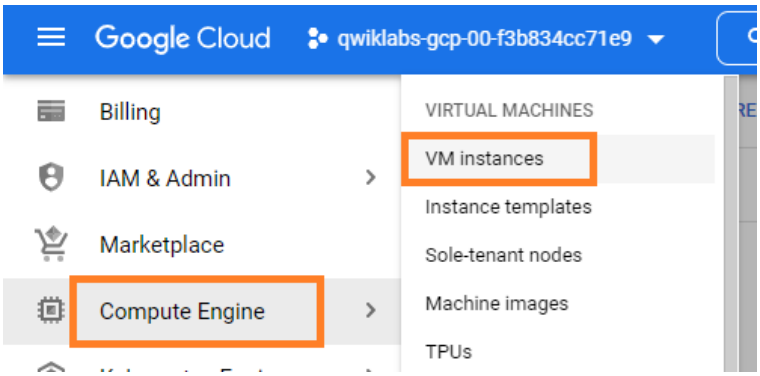


Segunda parte do laboratório.

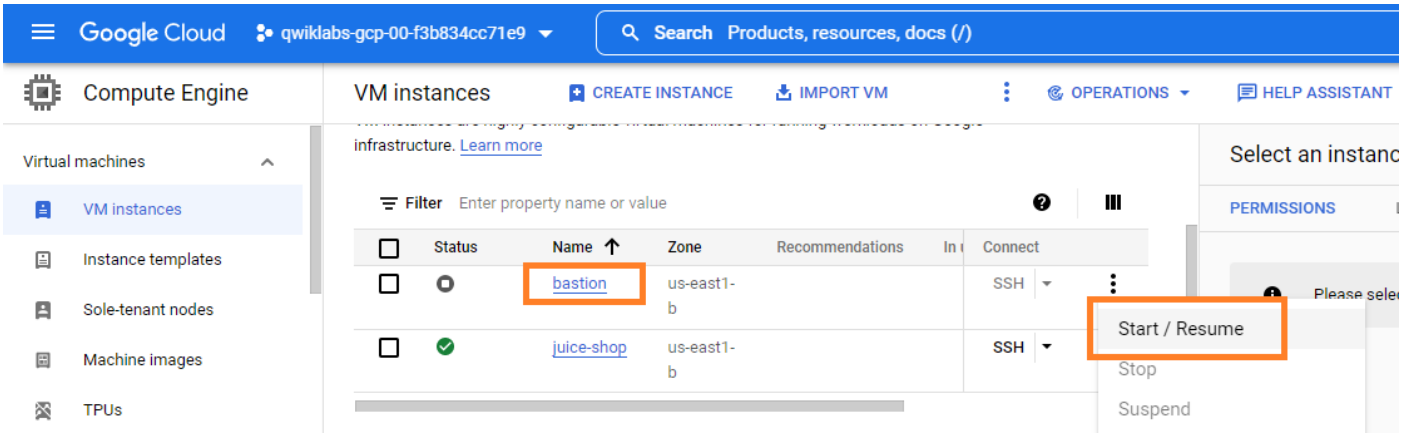
2. Acesse o Compute Engine no Console do Cloud e identifique o Bastion Host. A instância não deve estar em execução. Inicie a instância.



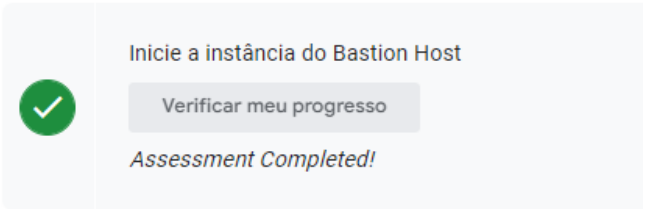
No menu lateral, procure por “Compute engine” e depois clique em “VM instances”



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



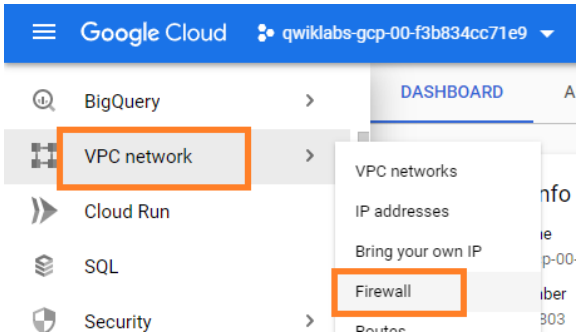
Após isso, aguarde o processo e valide a segunda parte.



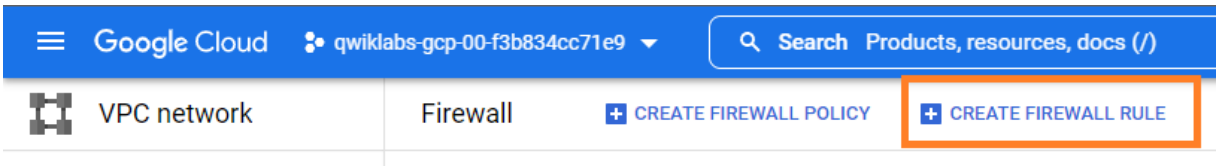
Terceira parte:

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-ql-528` .

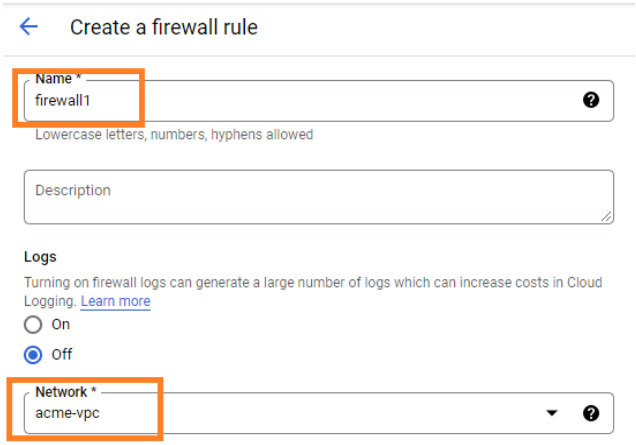
Volte no menu da esquerda em “VPC network” e depois clique em “Firewall”.



Depois clique em “Create firewall rule”



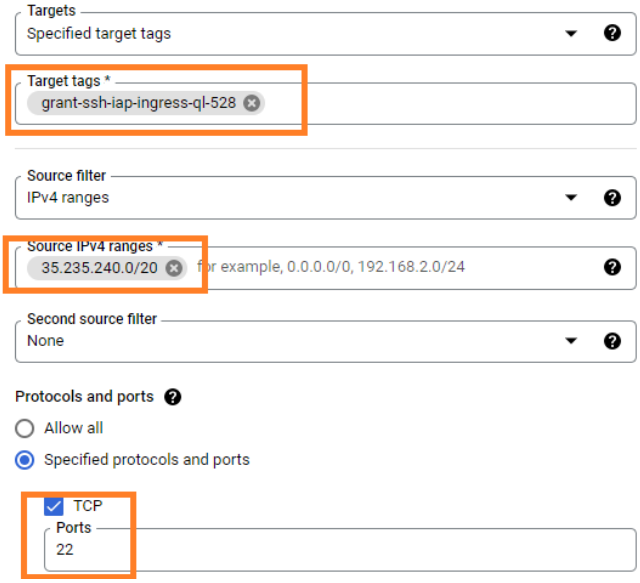
Preencha um nome a sua escolha e depois selecione clique no campo “Network” e selecione a rede que já está na listagem.



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

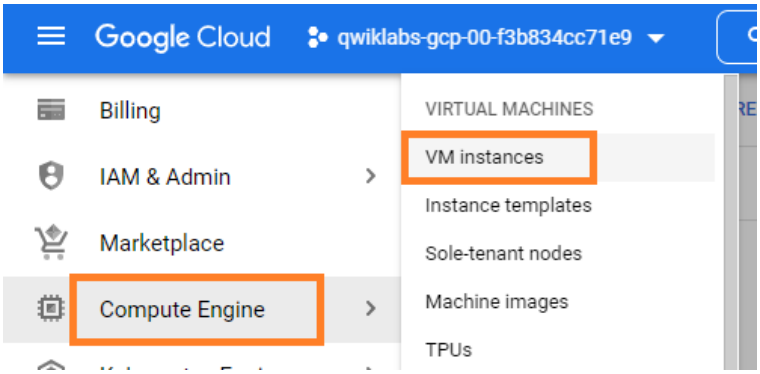
No campo “Source IPv4 ranges” informe o valor **35.235.240.0/20**.

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

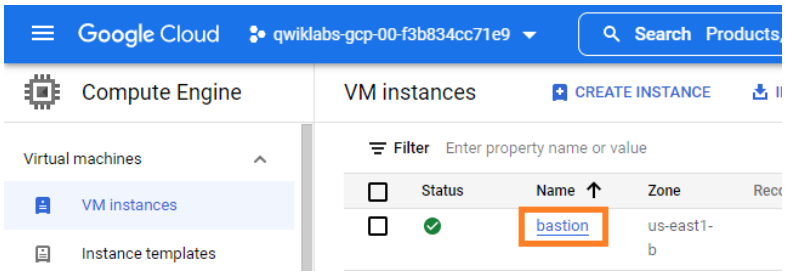


Depois clique em “Create” ao final da página.

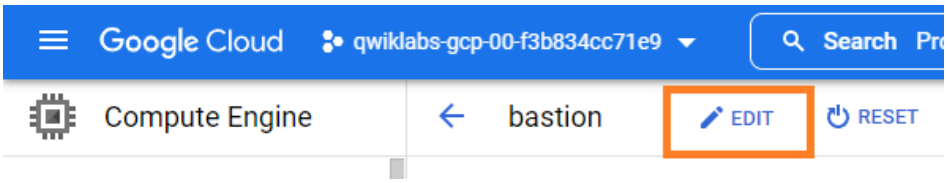
Volte no menu da esquerda em “Compute engine” e depois clique em “VM instances”



Clique sobre o nome da instância “bastion”



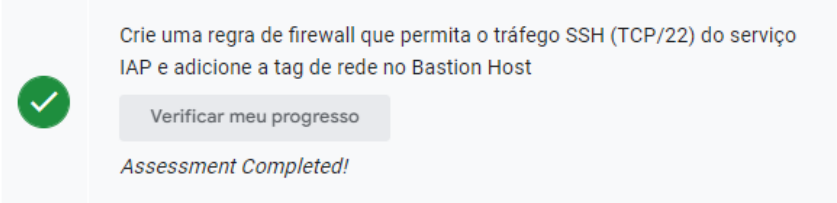
Depois clique sobre o botão “Edit” na faixa azul acima da tela.



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.

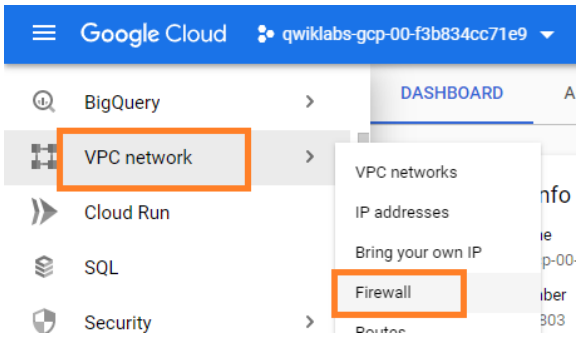
Aguarde o processo e depois valide a terceira parte do laboratório.



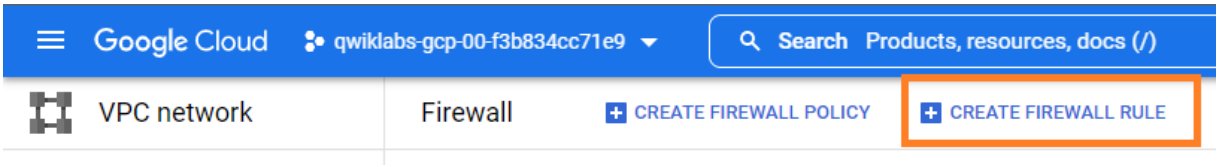
Quarta parte

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”

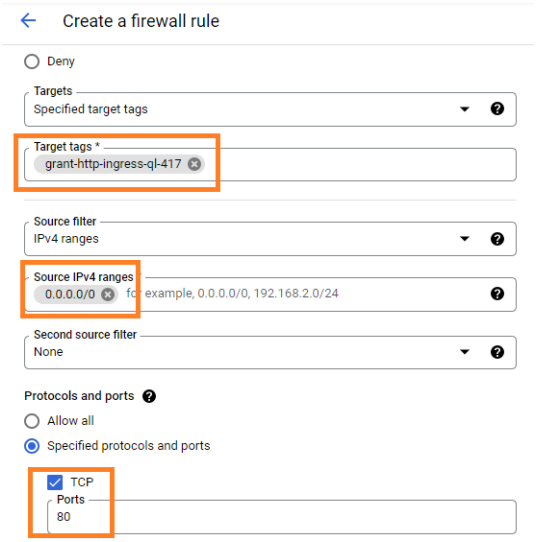


Preencha um nome a sua escolha e depois selecione clique no campo “Network” e selecione a rede que já está na listagem.

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

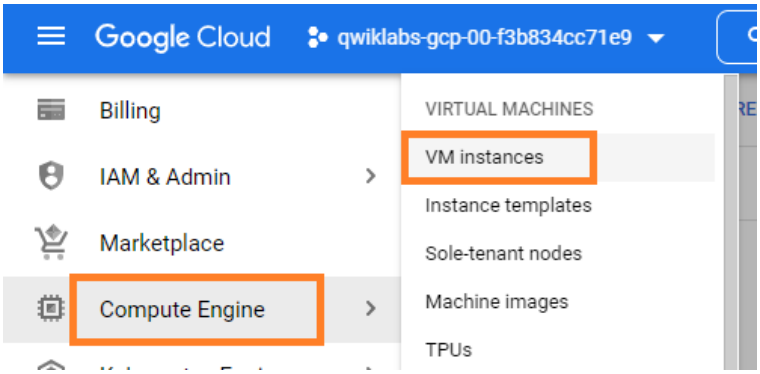
No campo “Source IPv4 ranges” informe o valor **0.0.0.0/0**.

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

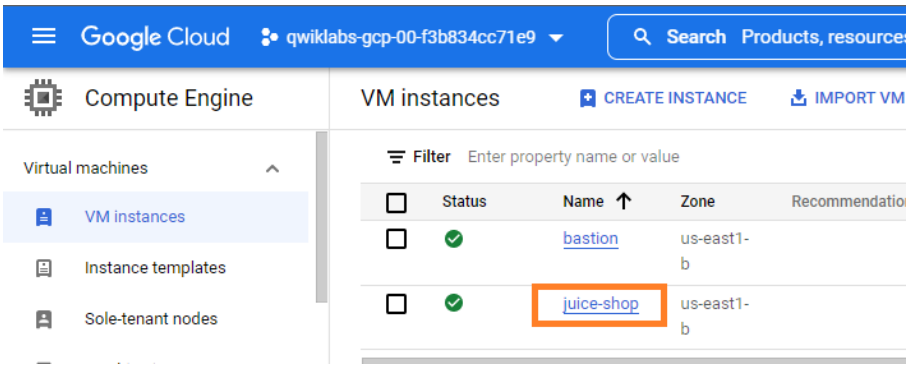


Clique em “Create” ao final da página.

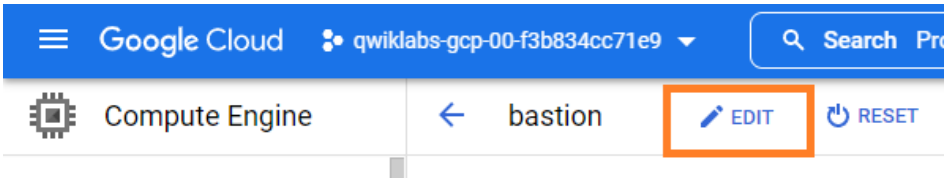
Volte no menu da esquerda em “Compute engine” e depois clique em “VM instances”



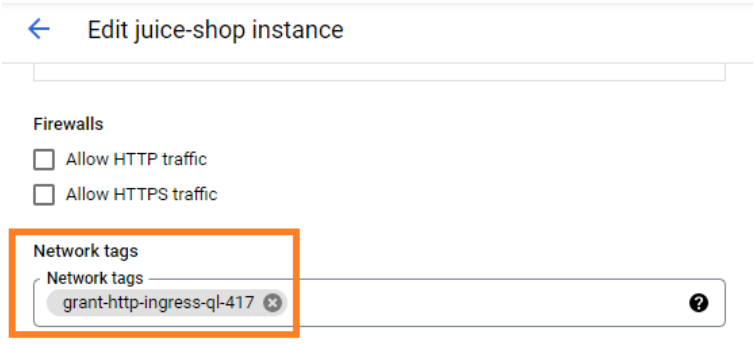
Clique sobre o nome da instância “juice-shop”



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

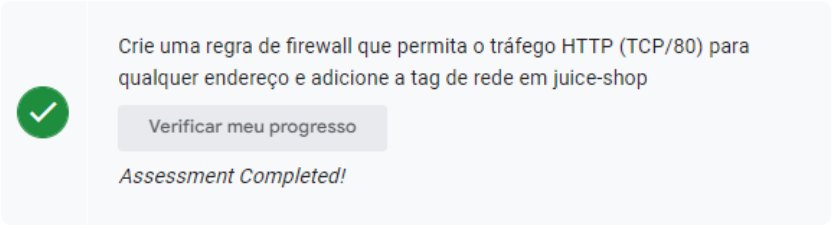


Desça na tela até encontrar a categoria “Network” e no campo “Network tags” informe o mesmo nome que seu laboratório indicou, o qual foi usado na etapa anterior.



Clique em “Save” ao final da página.

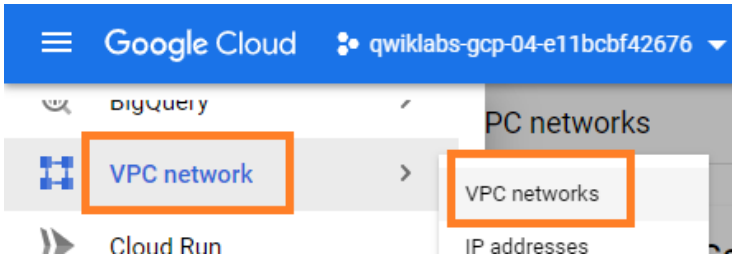
Volte para validar a quarta parte



Quinta parte

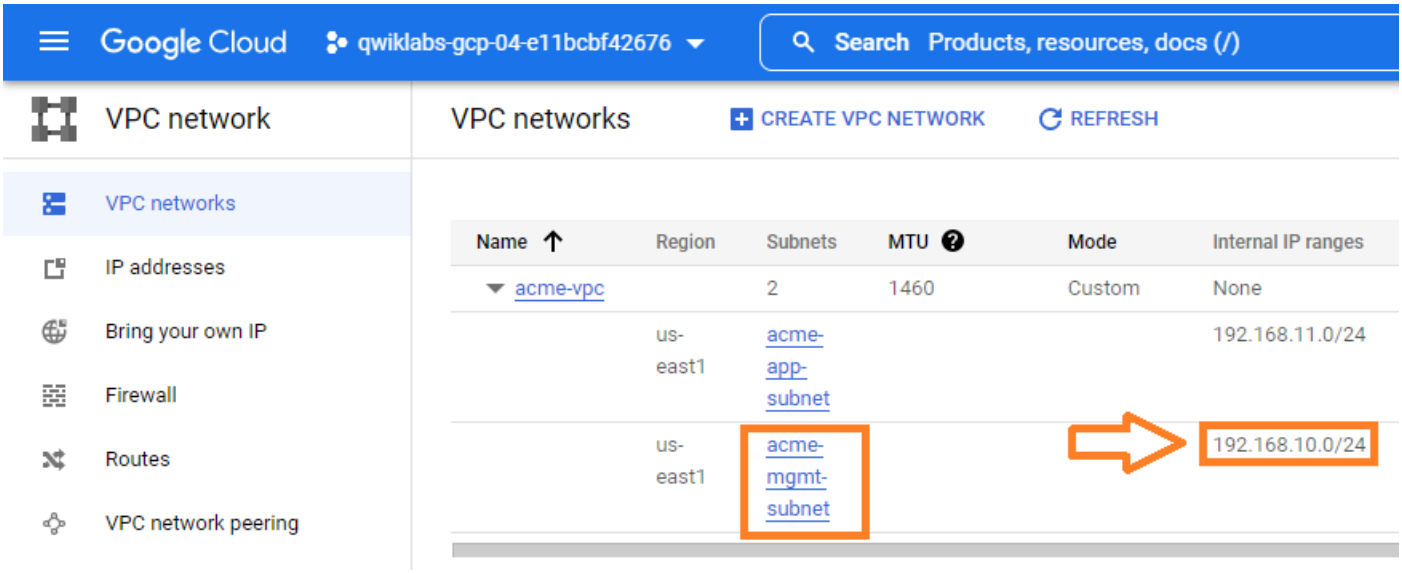
5. Você precisa se conectar a `juice-shop` no Bastion Host usando SSH. Crie uma regra de firewall que permita o tráfego SSH (TCP/22) do endereço de rede `acme-mgmt-subnet`. Ela precisa ser ativada na instância de `juice-shop` usando uma tag de rede de `grant-ssh-internal-ingress-ql-767` .

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

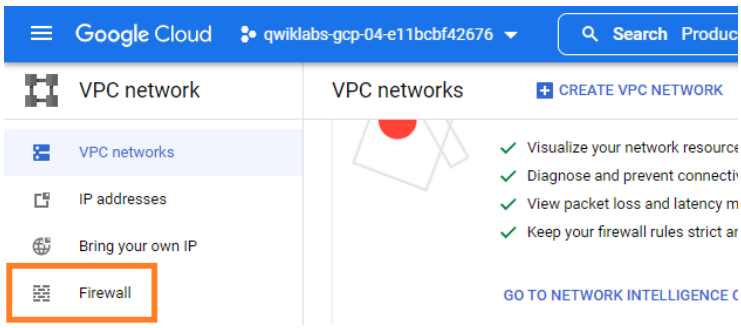


Procure pela rede que foi indicada no seu laboratório.

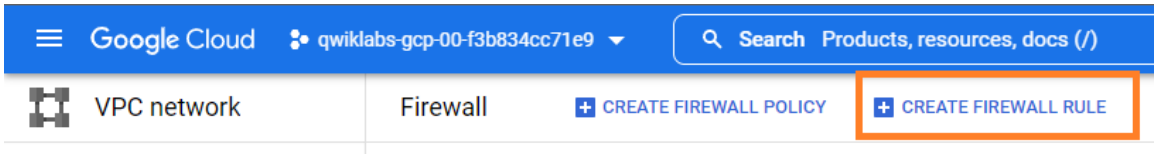
Copie o valor do IP indicado pela seta. Guarde esse valor anotado em algum lugar.



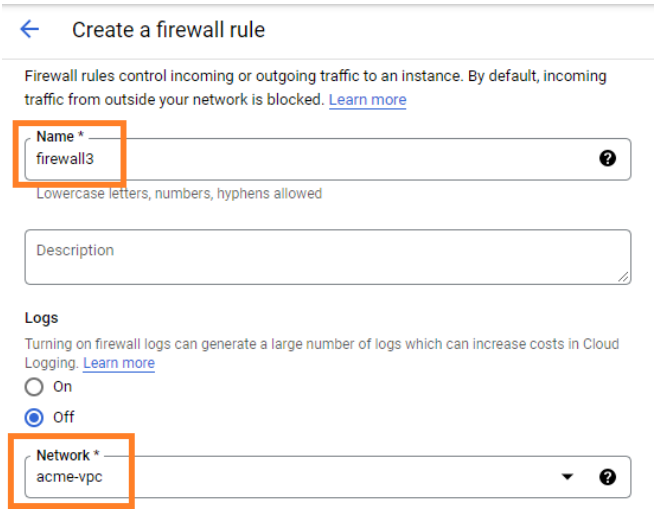
Volte no menu da esquerda e clique em “Firewall”.



Depois clique em “Create firewall rule”



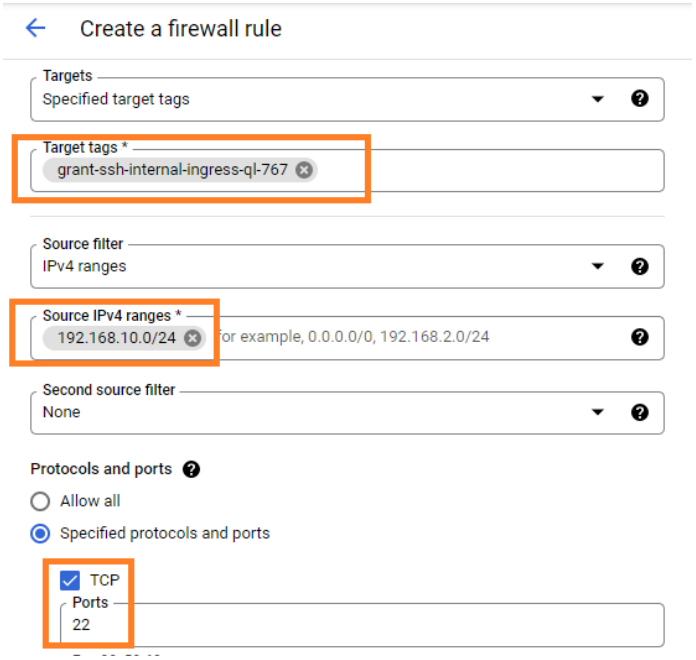
Preencha um nome a sua escolha e depois selecione clique no campo “Network” e selecione a rede que já está na listagem.



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

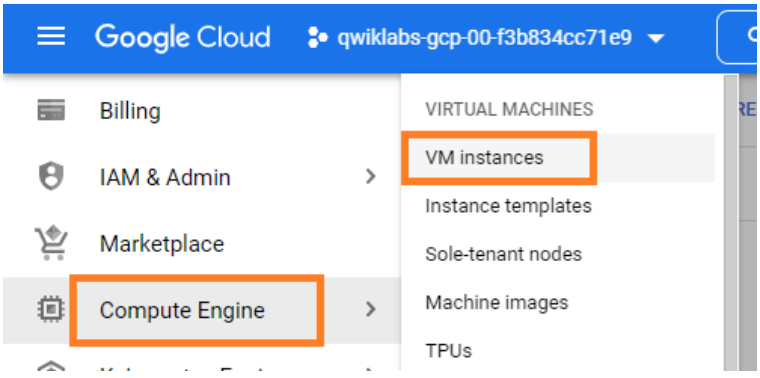
No campo “Source IPv4 ranges” informe o valor do IP de acme-mgmt-subnet que foi copiado na etapa anterior.

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

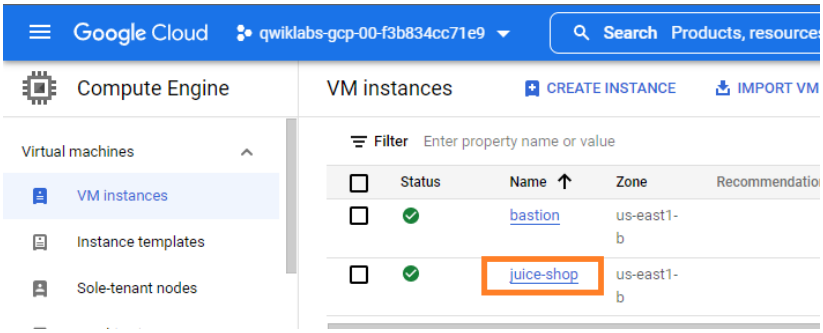


Clique em “Create” ao final da tela.

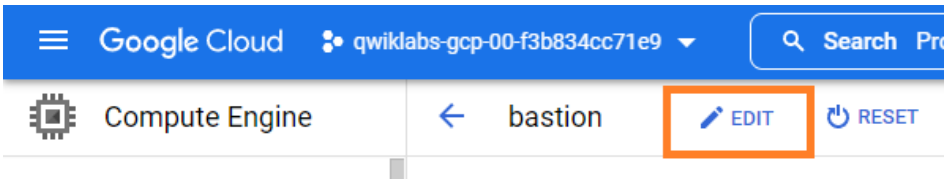
Volte no menu da esquerda em “Compute engine” e depois clique em “VM instances”



Clique sobre o nome da instância “juice-shop”



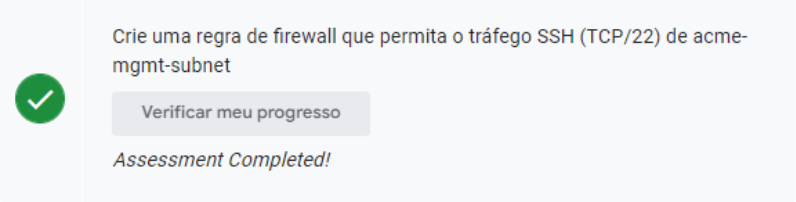
Depois clique sobre o botão “Edit” na faixa azul acima da tela.



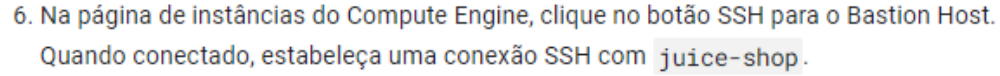
Desça na tela até encontrar a categoria “Network” e no campo “Network tags” adicione o mesmo nome que seu laboratório indicou, o qual foi usado na etapa anterior.

Clique em “Save” ao final da página.

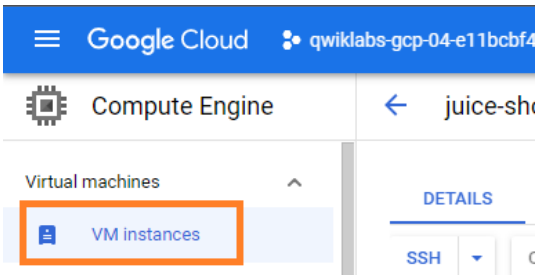
Volte para validar a quinta parte do laboratório.



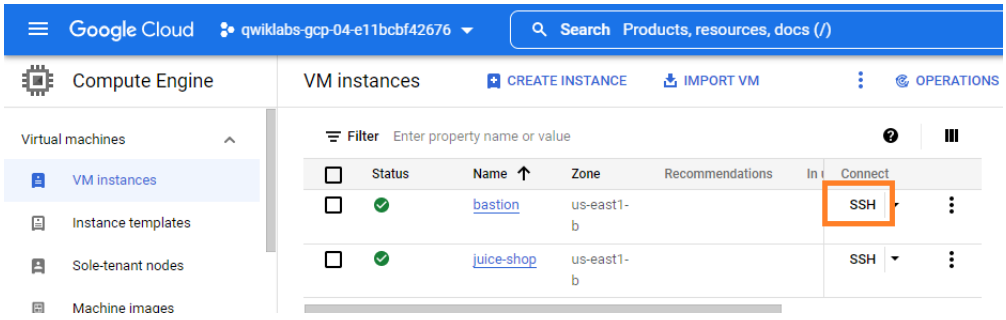
Sexta parte



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”



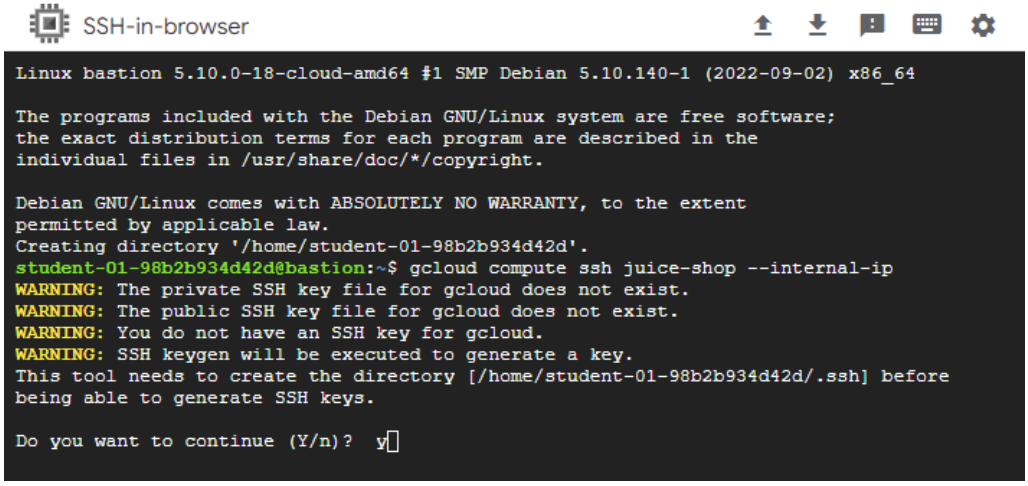
Uma nova tela irá se abrir.

Aguarde o carregamento dessa tela finalizar.

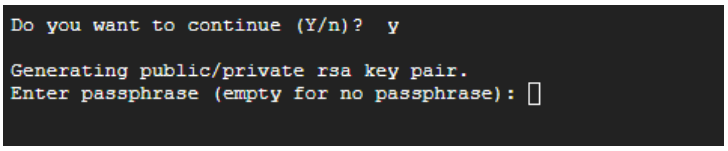
Após carregar digite o seguinte comando e depois aperte ENTER para executar.

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

Pressione “y” para confirmar e ENTER para continuar.

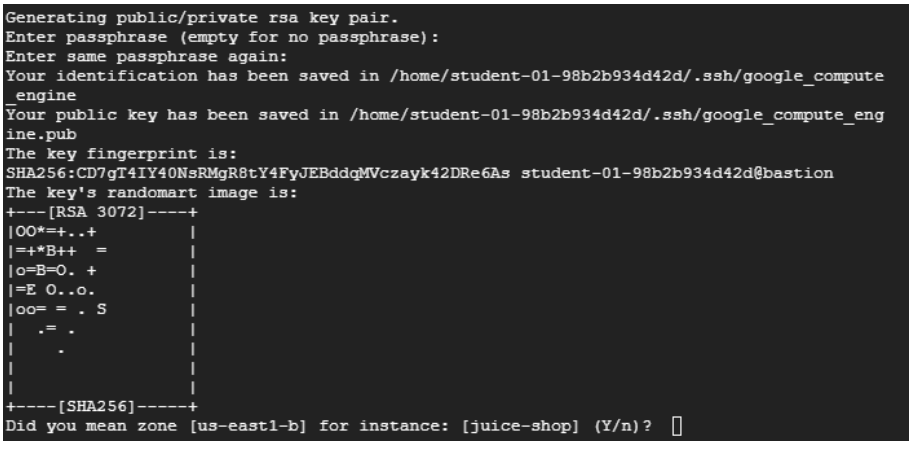


Quando aparecer a seguinte mensagem



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

A seguinte mensagem irá aparecer



Digite “y” e pressione ENTER.

Volte no laboratório e valide a última etapa