

Question 1 :

Step 1 :

Create a VPC network and a subnet from console,
Click Create VPC network.
Enter a Name of ketav-network1.
Under Subnets, set Subnet creation mode to Custom.
Enter a Name of ketav-us-central.
Select a Region of us-central1.
Enter an IP address range of 192.168.1.0/24.
Click Done.
Click Create.

Step 2 :

Create a bastion host for testing

Click the Create or Create instance button.
Specify a Name of bastion1 for your instance.
Set the Region to us-central1.
Set the Zone to us-central1-c.
Click the Management, security, disks, networking, sole tenancy link.
Click the Networking tab.
Under Network interfaces, click the pencil icon for the VM's default interface.
Set the Network to ketav-network1.
Set the Subnetwork to ketav-us-central.
Click Done.
Click the Create button to create and start the instance.

Step 3 :

Create a VM instance with no external IP

Click the Create button.
Specify a Name of nat-test1 for your instance.
Set the Region to us-central1.
Set the Zone to us-central1-c.
Click the Management, security, disks, networking, sole tenancy link.
Click the Networking tab.
Under Network interfaces, click the pencil icon for the VM's default interface.
Set the Network to ketav-network1.
Set the Subnetwork to ketav-us-central.
Set External IP to None.
Click Done.
Click the Create button to create and start the instance.

Step 4 :

Create firewall rule that allows connection

Click Create firewall rule.

Enter a Name of ketav-allow-ssh.

Specify a Network of ketav-network1.

Set Direction of traffic to ingress.

Set Action on match to allow.

Set Targets to All instances in the network.

Set Source filter to IP ranges.

Set Source IP ranges to 0.0.0.0/0.

Set Protocols and ports to Specified protocols and ports.

Select tcp and specify port 22.

Click Create.

Step 5 :

Give a network tag in bastion1 instance and allow secondary tag in ketav-network1 and enetr the same network tag.

Step 6 :

Login to nat-test1 to see we can reach internet

Connect bastion1 via ssh.

From bastion-1, connect to nat-test-1:

```
ssh nat-test-1 -A
```

From nat-test-1, attempt to connect to the Internet:

```
curl example.com
```

The screenshot shows a terminal window with the following commands and output:

```
ketav_bh@nat-test1: ~ - Google Chrome
ketav_bh@bastion1:~/.ssh$
ketav_bh@bastion1:~/.ssh$ cd ..
ketav_bh@bastion1:~$ ssh nat-test1 -A
ketav_bh@bastion1:~$ ssh nat-test1 -A
The authenticity of host 'nat-test1 (192.168.1.3)' can't be established.
ECDSA key fingerprint is SHA256:3KZjleTeoHJNSQjaajwoeIyDybWUr79q+3gwAQGR+Kk.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'nat-test1,192.168.1.3' (ECDSA) to the list of known hosts.
Permission denied (publickey).
ketav_bh@bastion1:~$ Connected, host fingerprint: ssh-rsa 0 3D:42:DC:64:96:96:7A:0B:2C:5E:86:89:37:85:B2:E4:F9:30:11:21:F7:BD:8E:63:4A:97:4A:3C:4B:06:4B
Linux bastion1 4.9.0-9-amd64 #1 SMP Debian 4.9.168-1+deb9u3 (2019-06-16) 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.
Last login: Mon Jul 22 07:55:59 2019 from 74.125.41.168
ketav_bh@nat-test1:~$ ssh nat-test1 -A
The authenticity of host 'nat-test1 (192.168.1.3)' can't be established.
ECDSA key fingerprint is SHA256:3KZjleTeoHJNSQjaajwoeIyDybWUr79q+3gwAQGR+Kk.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'nat-test1,192.168.1.3' (ECDSA) to the list of known hosts.
Linux nat-test1 4.9.0-9-amd64 #1 SMP Debian 4.9.168-1+deb9u3 (2019-06-16) 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.
ketav_bh@nat-test1:~$ curl example.com

curl: (7) Failed to connect to example.com port 80: Connection timed out
ketav_bh@nat-test1:~$
ketav_bh@nat-test1:~$
ketav_bh@nat-test1:~$
```

Step 7 :

Create a NAT configuration using cloud router.

Click Get started or Create NAT gateway.

Enter a Gateway name of nat-config.

Set the VPC network to ketav-network1.

Set the Region to us-central1.

Under Cloud Router, select Create new router.

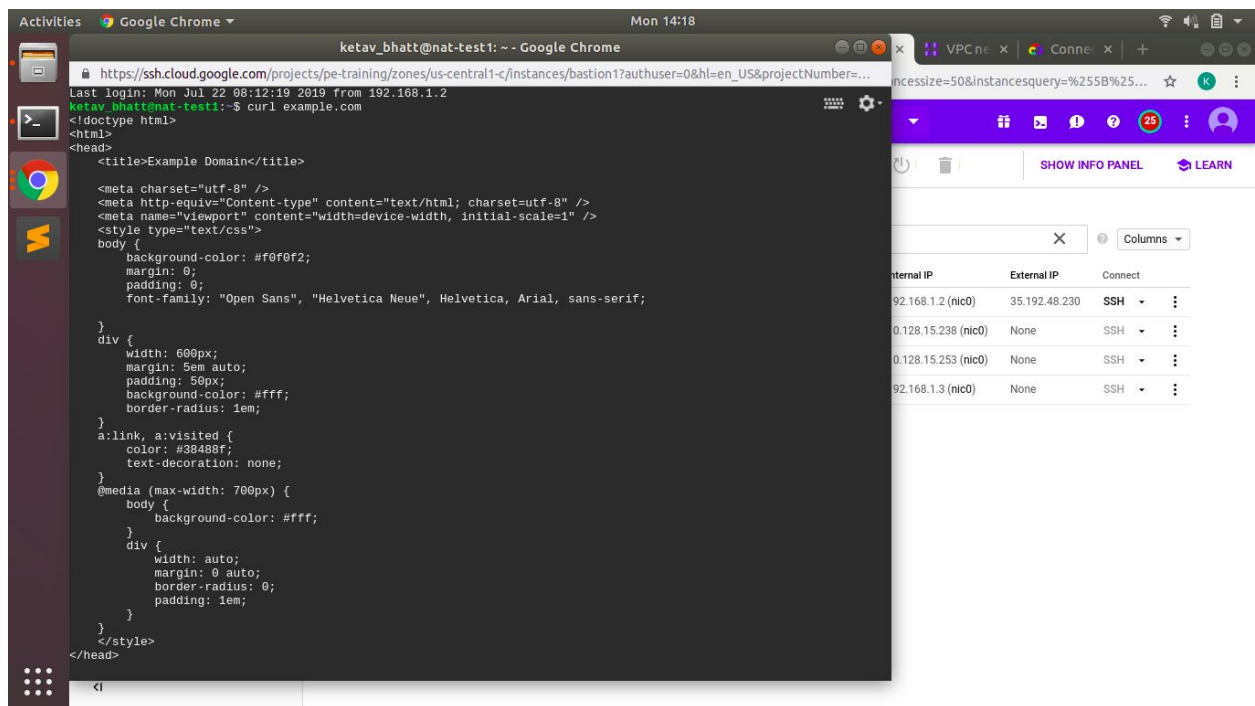
Enter a Name of nat-router.

Click Create.

Click Create.

Step 8 :

Attempt to connect to internet again from nat-test1



The screenshot shows a terminal window and a Google Chrome browser window. The terminal window displays the output of a curl command, showing an HTML page with a title 'Example Domain' and various CSS styles. The browser window shows a table of IP addresses and their connection status.

Internal IP	External IP	Connect
92.168.1.2 (nic0)	35.192.48.230	SSH
0.128.15.238 (nic0)	None	SSH
0.128.15.253 (nic0)	None	SSH
92.168.1.3 (nic0)	None	SSH