

Abdoul-Nourou Yigo  
Dr. Ziazen Zhou  
Cryptography and Cloud Security

## Assignment1

The following steps are the procedures used to accomplish the networking lab:

### **Setup and Requirement**

Setup project

```
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud config set project assignment1-230117
Updated property [core/project].
nouroudine@nouroudine-HP-PAVILION-Notebook:~$
```

Setup Zone

```
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud config set compute/zone us-central1-f
Updated property [compute/zone].
nouroudine@nouroudine-HP-PAVILION-Notebook:~$
```

### **Setup the environment**

Creating a Network named nw102

```
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute networks create nw102 --subnet-mode=custom
API [compute.googleapis.com] not enabled on project [864761210753].
Would you like to enable and retry (this will take a few minutes)?
(y/N)? y

Enabling service [compute.googleapis.com] on project [864761210753]...
Waiting for async operation operations/acf.61678ba5-4568-45f6-884c-9ed8f97a2054 to complete...
```

Operation is completed

```
gcloud help --sections PENDING
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute networks create nw102 --subnet-mode=custom
API [compute.googleapis.com] not enabled on project [864761210753].
Would you like to enable and retry (this will take a few minutes)?
(y/N)? y

Enabling service [compute.googleapis.com] on project [864761210753]...
Waiting for async operation operations/acf.61678ba5-4568-45f6-884c-9ed8f97a2054 to complete...
Operation finished successfully. The following command can describe the Operation details:
  gcloud services operations describe operations/tmo-acf.61678ba5-4568-45f6-884c-9ed8f97a2054
Created [https://www.googleapis.com/compute/v1/projects/assignment1-230117/global/networks/nw102].
NAME  SUBNET_MODE  BGP_ROUTING_MODE  IPV4_RANGE  GATEWAY_IPV4
nw102  CUSTOM      REGIONAL        10.128.0.0/16  10.128.0.1
```

Instances on this network will not be reachable until firewall rules are created. As an example, you can allow all internal traffic between instances as well as SSH, RDP, and ICMP by running:

```
$ gcloud compute firewall-rules create <FIREWALL_NAME> --network nw102 --allow tcp,udp,icmp --source-ranges <IP_RANGE>
$ gcloud compute firewall-rules create <FIREWALL_NAME> --network nw102 --allow tcp:22,tcp:3389,icmp
```

## Creating a network range

```
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute networks subnets create nw102-us --network nw102 --range 192.168.10.0/24 --region us-central1
Created [https://www.googleapis.com/compute/v1/projects/assignment1-230117/regions/us-central1/subnetworks/nw102-us].
NAME      REGION    NETWORK   RANGE
nw102-us  us-central1  nw102   192.168.10.0/24
nouroudine@nouroudine-HP-PAVILION-Notebook:~$
```

## Option to subnetwork in other regions

```
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute networks subnets create nw102-eu
--network nw102 --range 192.168.20.0/24

For the following subnetwork:
- [nw102-eu]
choose a region:
[1] asia-east1
[2] asia-east2
[3] asia-northeast1
[4] asia-south1
[5] asia-southeast1
[6] australia-southeast1
[7] europe-north1
[8] europe-west1
[9] europe-west2
[10] europe-west3
[11] europe-west4
[12] northamerica-northeast1
[13] southamerica-east1
[14] us-central1
[15] us-east1
[16] us-east4
[17] us-west1
[18] us-west2
Please enter your numeric choice: Please enter a value between 1 and 18: ■
```

## Operation succeeded

```
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute networks subnets create nw102-eu
--network nw102 --range 192.168.20.0/24
```

For the following subnetwork:

- [nw102-eu]

choose a region:

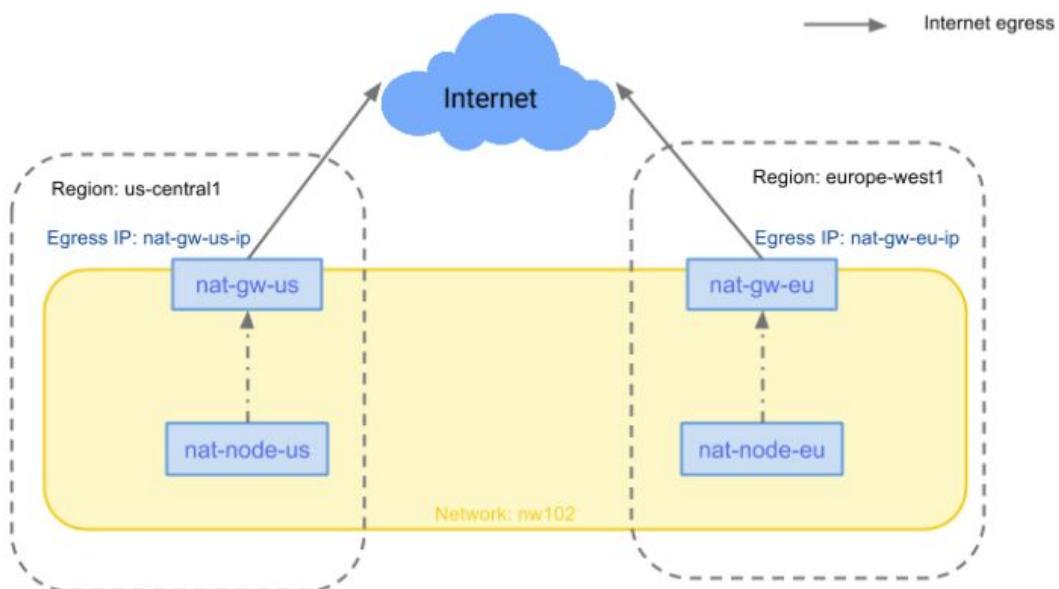
- [1] asia-east1
- [2] asia-east2
- [3] asia-northeast1
- [4] asia-south1
- [5] asia-southeast1
- [6] australia-southeast1
- [7] europe-north1
- [8] europe-west1
- [9] europe-west2
- [10] europe-west3
- [11] europe-west4
- [12] northamerica-northeast1
- [13] southamerica-east1
- [14] us-central1
- [15] us-east1
- [16] us-east4
- [17] us-west1
- [18] us-west2

## Creating firewalls rules:

```
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute firewall-rules create nw102-allow-internal --network nw102 --source-ranges 192.168.10.0/24,192.168.20.0/24 --allow tcp,udp,icmp
Creating firewall...done.
NAME          NETWORK DIRECTION PRIORITY ALLOW      DENY    DISABLED
nw102-allow-internal nw102  INGRESS   1000    tcp,udp,icmp  False
nouroudine@nouroudine-HP-PAVILION-Notebook:~$
```

## Creating a NAT gateway

NAT architecture in both regions



## Create VMs in several regions

Create NAT gateways in the U.S and EU

```
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute addresses create nat-gw-us-ip --region us-central1
Created [https://www.googleapis.com/compute/v1/projects/assignment1-230117/regions/us-central1/addresses/nat-gw-us-ip].
nouroudine@nouroudine-HP-PAVILION-Notebook:~$
```

```
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute addresses create nat-gw-eu-ip --region europe-west1
Created [https://www.googleapis.com/compute/v1/projects/assignment1-230117/regions/europe-west1/addresses/nat-gw-eu-ip].
nouroudine@nouroudine-HP-PAVILION-Notebook:~$
```

## Creating different virtual machines using different systems

```
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute instances create nat-gw-us --network nw102 --subnet nw102-us --address nat-gw-us-ip --can-ip-forward --zone us-central1-f --image-family debian-9 --image-project debian-cloud
Created [https://www.googleapis.com/compute/v1/projects/assignment1-230117/zones/us-central1-f/instances/nat-gw-us].
^LNAME      ZONE      MACHINE_TYPE      PREEMPTIBLE      INTERNAL_IP      EXTERNAL_IP      STATUS
nat-gw-us  us-central1-f  n1-standard-1           192.168.10.2  35.192.73.232  RUNNING
nouroudine@nouroudine-HP-PAVILION-Notebook:~$
```

The screenshot shows the Google Cloud Platform Compute Engine interface. On the left, there's a sidebar with options like VM instances, Instance groups, Instance templates, Sole tenant nodes, Disks, and Snapshots. The main area is titled 'VM instances' and contains a table with columns: Name, Zone, Recommendation, Internal IP, External IP, and Connect. Two instances are listed: 'nat-gw-us' in 'us-central1-f' zone and 'nat-gw-eu' in 'europe-west1-c' zone. Both instances have green status indicators and are running.

Name	Zone	Recommendation	Internal IP	External IP	Status
nat-gw-us	us-central1-f		192.168.10.2 (nic0)	35.192.73.232	SSH RUNNING
nat-gw-eu	europe-west1-c		192.168.20.2 (nic0)	35.240.114.41	SSH RUNNING

```
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute instances create nat-gw-eu --network nw102 --subnet nw102-eu --address nat-gw-eu-ip --can-ip-forward --zone europe-west1-c --image-family centos-7 --image-project centos-cloud
Created [https://www.googleapis.com/compute/v1/projects/assignment1-230117/zones/europe-west1-c/instances/nat-gw-eu].
^LNAME      ZONE      MACHINE_TYPE      PREEMPTIBLE      INTERNAL_IP      EXTERNAL_IP      STATUS
nat-gw-eu  europe-west1-c  n1-standard-1           192.168.20.2  35.240.114.41  RUNNING
nouroudine@nouroudine-HP-PAVILION-Notebook:~$
```

This screenshot shows the same Compute Engine interface as the previous one, but with three instances listed in the table: 'nat-gw-eu', 'nat-gw-us', and 'nat-node-us'. The 'nat-node-us' instance is new and has not yet started.

Name	Zone	Recommendation	Internal IP	External IP	Status
nat-gw-eu	europe-west1-c		192.168.20.2 (nic0)	35.240.114.41	SSH RUNNING
nat-gw-us	us-central1-f		192.168.10.2 (nic0)	35.192.73.232	SSH RUNNING
nat-node-us	us-central1-f				SSH STOPPED

## Instances without --can-ip-forward

```
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute instances create nat-node-us --network nw102 --subnet nw102-us --zone us-central1-f --image-family debian-9 --image-project debian-cloud
^LNAME      ZONE      MACHINE_TYPE      PREEMPTIBLE      INTERNAL_IP      EXTERNAL_IP      STATUS
nat-node-us  us-central1-f  n1-standard-1           192.168.10.3  35.192.73.233  STOPPED
nouroudine@nouroudine-HP-PAVILION-Notebook:~$
```

The screenshot shows the Compute Engine interface again, with the 'nat-node-us' instance now listed as 'STOPPED' in the status column. The other two instances remain running.

Name	Zone	Recommendation	Internal IP	External IP	Status
nat-gw-eu	europe-west1-c		192.168.20.2 (nic0)	35.240.114.41	SSH RUNNING
nat-gw-us	us-central1-f		192.168.10.2 (nic0)	35.192.73.232	SSH RUNNING
nat-node-us	us-central1-f				STOPPED

```
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute instances create nat-node-eu --network nw102 --subnet nw102-eu --zone europe-west1-c --image-family centos-7 --image-project centos-cloud --no-address
Created [https://www.googleapis.com/compute/v1/projects/assignment1-230117/zones/europe-west1-c/instances/nat-node-eu].
NAME          ZONE      MACHINE_TYPE  PREEMPTIBLE INTERNAL_IP  EXTERNAL_IP STATUS
nat-node-eu   europe-west1-c  n1-standard-1    192.168.20.3        RUNNING
nouroudine@nouroudine-HP-PAVILION-Notebook:~$
```

Name	Zone	Recommendation	Internal IP	External IP	Connect
nat-gw-eu	europe-west1-c		192.168.20.2 (nic0)	35.240.114.41	SSH
nat-gw-us	us-central1-f		192.168.10.2 (nic0)	35.192.73.232	SSH
nat-node-eu	europe-west1-c		192.168.20.3 (nic0)	None	SSH
nat-node-us	us-central1-f		192.168.10.3 (nic0)	35.224.86.177	SSH

## Allowing connection by SSH

```
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute firewall-rules create nw102-allow-ssh --network nw102 --source-ranges 0.0.0.0/0 --allow tcp:22
Creating firewall...:Created [https://www.googleapis.com/compute/v1/projects/assignment1-230117/global/firewalls/nw102-allow-ssh].
Creating firewall...done.
NAME          NETWORK DIRECTION PRIORITY ALLOW DENY DISABLED
nw102-allow-ssh nw102  INGRESS  1000   tcp:22     False
nouroudine@nouroudine-HP-PAVILION-Notebook:~$
```

## Series of SSH connections to instances

```
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute ssh nat-gw-us --zone us-central1-f
Updating project ssh metadata...:Updated [https://www.googleapis.com/compute/v1/projects/assignment1-230117].
Updating project ssh metadata...done.
Waiting for SSH key to propagate.
Warning: Permanently added 'compute.6878298777082202584' (ECDSA) to the list of known hosts.
Linux nat-gw-us 4.9.0-8-amd64 #1 SMP Debian 4.9.130-2 (2018-10-27) 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.
nouroudine@nat-gw-us:~$
```

```
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute ssh nat-gw-eu --zone europe-west1-c
Warning: Permanently added 'compute.392086308224042779' (ECDSA) to the list of known hosts.
[nouroudine@nat-gw-eu ~]$
```

```
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute ssh nat-node-us --zone us-central1-f
Warning: Permanently added 'compute.1211501300194049062' (ECDSA) to the list of known hosts.
Linux nat-node-us 4.9.0-8-amd64 #1 SMP Debian 4.9.130-2 (2018-10-27) 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.
```

## Deleting instance

```
[gcloud compute instances delete-access-config] [https://www.googleapis.com/compute/v1/projects/assignment1-230117/zones/us-central1-f/instances/nat-node-us].  
nouroudine@nouroudine-HP-PAVILION-Notebook:~$
```

## SSH failed after instance deletion

```
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute ssh nat-node-us --zone us-central1-f  
ERROR: (gcloud.compute.ssh) Instance [nat-node-us] in zone [us-central1-f] does not have an external IP address, so you cannot SSH into it. To add an external IP address to the instance, use [gcloud compute instances add-access-config].  
nouroudine@nouroudine-HP-PAVILION-Notebook:~$
```

## Set up NAT

### Separates instances into two partitions

```
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute instances add-tags nat-node-us --zone us-central1-f --tags nat-us  
Updated [https://www.googleapis.com/compute/v1/projects/assignment1-230117/zones/us-central1-f/instances/nat-node-us].  
nouroudine@nouroudine-HP-PAVILION-Notebook:~$
```

```
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute instances add-tags nat-node-eu --zone europe-west1-c --tags nat-eu  
Updated [https://www.googleapis.com/compute/v1/projects/assignment1-230117/zones/europe-west1-c/instances/nat-node-eu].  
nouroudine@nouroudine-HP-PAVILION-Notebook:~$
```

```
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute routes create nw102-nat-us --network nw102 --tags nat-us --destination-range 0.0.0.0/0 --next-hop-instance nat-gw-us --next-hop-instance-zone us-central1-f --priority 800  
Created [https://www.googleapis.com/compute/v1/projects/assignment1-230117/global/routes/nw102-nat-us].  
WARNING: Some requests generated warnings:  
- Next hop instance 'https://www.googleapis.com/compute/v1/projects/assignment1-230117/zones/us-central1-f/instances/nat-gw-us' does not exist.  
NAME NETWORK DEST_RANGE NEXT_HOP PRIORITY  
nw102-nat-us nw102 0.0.0.0/0 us-central1-f/instances/nat-gw-us 800  
nouroudine@nouroudine-HP-PAVILION-Notebook:~$
```

```
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute routes create nw102-nat-eu --network nw102 --tags nat-eu --destination-range 0.0.0.0/0 --next-hop-instance nat-gw-eu --next-hop-instance-zone europe-west1-c --priority 800
Created [https://www.googleapis.com/compute/v1/projects/assignment1-230117/global/routes/nw102-nat-eu].
NAME          NETWORK  DEST_RANGE   NEXT_HOP           PRIORITY
nw102-nat-eu  nw102    0.0.0.0/0   europe-west1-c/instances/nat-gw-eu  800
nouroudine@nouroudine-HP-PAVILION-Notebook:~$
```

Make sure traffic through NAT gateways gets forwarded and NATed to its own IP

SSH in the machine in us-central1-f to do some configuration

```
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute ssh nat-gw-us --zone us-central1-f
Linux nat-gw-us 4.9.0-8-amd64 #1 SMP Debian 4.9.130-2 (2018-10-27) 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: Wed Jan 30 02:11:20 2019 from 47.34.9.131
nouroudine@nat-gw-us:~$
```

```
nouroudine@nat-gw-us:~$ echo 1 | sudo tee /proc/sys/net/ipv4/ip_forward
1
nouroudine@nat-gw-us:~$
```

```
nouroudine@nat-gw-us:~$ sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
nouroudine@nat-gw-us:~$
```

SSH in the machine in europe-west1-c do achieve some configurations

```
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute ssh nat-gw-eu --zone europe-west1-c
Last login: Wed Jan 30 02:13:40 2019 from 47.34.9.131
[nouroudine@nat-gw-eu ~]$
```

```
Last login: Wed Jan 30 02:13:40 2019 from 47.34.9.131
[nouroudine@nat-gw-eu ~]$ echo 1 | sudo tee /proc/sys/net/ipv4/ip_forward
1
[nouroudine@nat-gw-eu ~]$ █
```

```
x - □ nouroudine@nat-gw-eu:~
[nouroudine@nat-gw-eu ~]$ sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
[nouroudine@nat-gw-eu ~]$ █
```

## SSH NAted instances to verify NAT configuration

```
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute ssh nat-gw-us --zone us-central1-f
Linux nat-gw-us 4.9.0-8-amd64 #1 SMP Debian 4.9.130-2 (2018-10-27) 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: Wed Jan 30 03:40:01 2019 from 47.34.9.131
nouroudine@nat-gw-us:~$ █
```

## SSH an instance from another instance using the NAT configuration

Permission denied at first tried

```
nouroudine@nat-gw-us:~$ ssh nat-node-us
The authenticity of host 'nat-node-us (192.168.10.6)' can't be established.
ECDSA key fingerprint is SHA256:QHu7hdIB51T0tuvLk/Y/R0wUS4ccMtnTmjzc9EBrjaY.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'nat-node-us,192.168.10.6' (ECDSA) to the list of known hosts.
Permission denied (publickey).
nouroudine@nat-gw-us:~$ █
```

Used the right configuration to have permission

```
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ ssh-add ~/.ssh/google_compute_engine
Enter passphrase for /home/nouroudine/.ssh/google_compute_engine:
Identity added: /home/nouroudine/.ssh/google_compute_engine (/home/nouroudine/.ssh/google_com
ute_engine)
nouroudine@nouroudine-HP-PAVILION-Notebook:~$
```

Now the operation was successful

```
nouroudine@nat-gw-us:~$ ssh nat-node-us
Linux nat-node-us 4.9.0-8-amd64 #1 SMP Debian 4.9.130-2 (2018-10-27) 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.
nouroudine@nat-node-us:~$
```

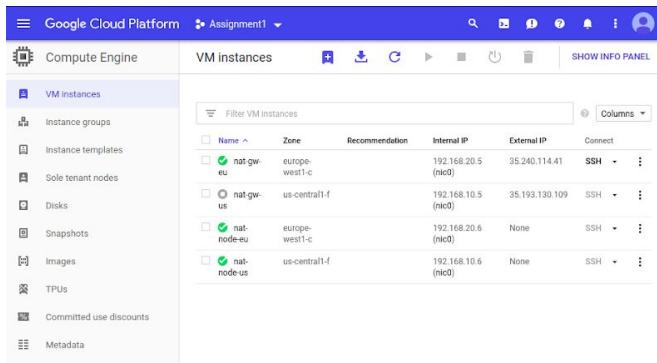
The Traceroute is not working because the packet is not installed. After installing the package on Centos-7 and debian-9, I was able to run the command on Google.com.

```
[nouroudine@nat-gw-eu ~]$ traceroute google.com
traceroute to google.com (66.102.1.100), 30 hops max, 60 byte packets
 1 * * *
 2 * * *
 3 * * *
 4 * * *
 5 * * *
 6 * * *
 7 * * *
 8 * * *
 9 * * *
10 wb-in-f100.1e100.net (66.102.1.100)  0.726 ms  0.689 ms  0.796 ms
```



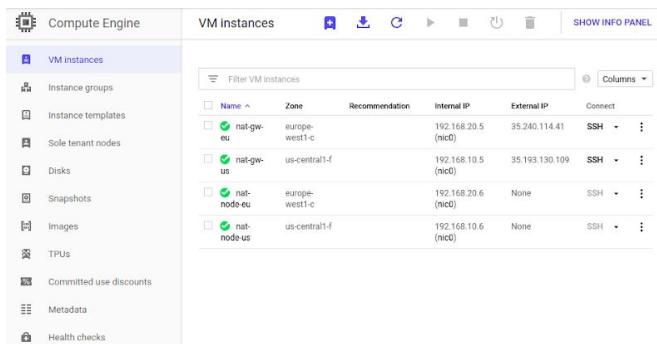
## Restarting the NAT gateway

### Stop the instance



```
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute instances stop nat-gw-us --zone us-central1-f
Logout
Connection to 35.193.130.109 closed.
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute instances stop nat-gw-us --zone us-central1-f
Stopping instance(s) nat-gw-us...done.
Updated [https://www.googleapis.com/compute/v1/projects/assignment1-230117/zones/us-central1-f/instances/nat-gw-us].
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ 
```

### Start the instance



```
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute instances stop nat-gw-us --zone us-central1-f
Stopping instance(s) nat-gw-us...done.
Updated [https://www.googleapis.com/compute/v1/projects/assignment1-230117/zones/us-central1-f/instances/nat-gw-us].
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute instances start nat-gw-us --zone us-central1-f
Starting instance(s) nat-gw-us...done.
Updated [https://www.googleapis.com/compute/v1/projects/assignment1-230117/zones/us-central1-f/instances/nat-gw-us].
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ 
```

## Applying the startup scripts before restarting the NAT gateways

```
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute instances add-metadata nat-gw-us
--zone us-central1-f --metadata startup-script=\
> "#! /bin/bash
> sh -c \'echo 1 > /proc/sys/net/ipv4/ip_forward\'
> iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE"
Updated [https://www.googleapis.com/compute/v1/projects/assignment1-230117/zones/us-central1-f/instances/nat-gw-us].
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ 
```

```
, instances/nat-gw-us].
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute instances stop nat-gw-us --zone us-central1-f
Stopping instance(s) nat-gw-us...done.
Updated [https://www.googleapis.com/compute/v1/projects/assignment1-230117/zones/us-central1-f/instances/nat-gw-us].
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ █
```

```
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute instances start nat-gw-us --zone us-central1-f
Starting instance(s) nat-gw-us...done.
Updated [https://www.googleapis.com/compute/v1/projects/assignment1-230117/zones/us-central1-f/instances/nat-gw-us].
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ █
```

```
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute instances add-metadata nat-gw-eu --zone europe-west1-c --metadata start-script=\
> "#! /bin/bash
> sh -c \"echo 1 > /proc/sys/net/ipv4/ip_forward\"
> iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE"
Updated [https://www.googleapis.com/compute/v1/projects/assignment1-230117/zones/europe-west1-c/instances/nat-gw-eu].
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ █
```

```
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute instances stop nat-gw-eu --zone europe-west1-c
Stopping instance(s) nat-gw-eu...done.
Updated [https://www.googleapis.com/compute/v1/projects/assignment1-230117/zones/europe-west1-c/instances/nat-gw-eu].
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ █
```

```
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute instances start nat-gw-eu --zone europe-west1-c
Starting instance(s) nat-gw-eu...done.
Updated [https://www.googleapis.com/compute/v1/projects/assignment1-230117/zones/europe-west1-c/instances/nat-gw-eu].
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ █
```

## Optimal - Reduce NAT external exposure

```
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute firewall-rules delete nw102-allow-ssh
Deleted [https://www.googleapis.com/compute/v1/projects/assignment1-230117/global/firewalls/nw102-allow-ssh].
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ █
```

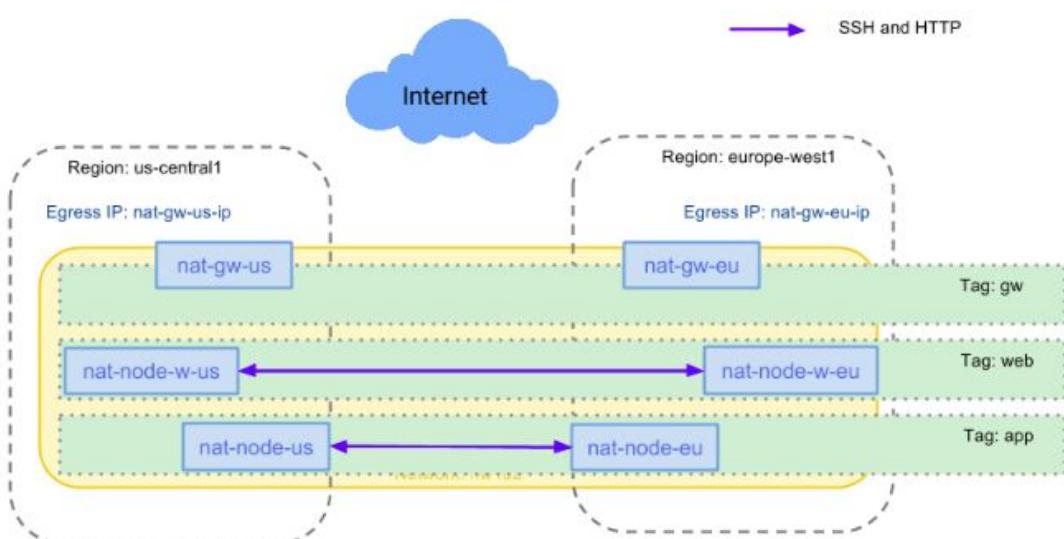
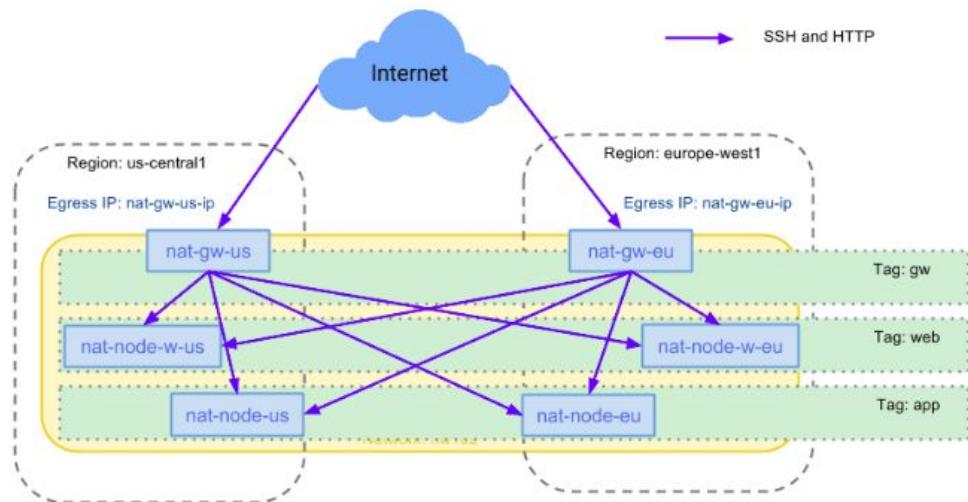
Restrict Current SSH to current machine ( my machine )

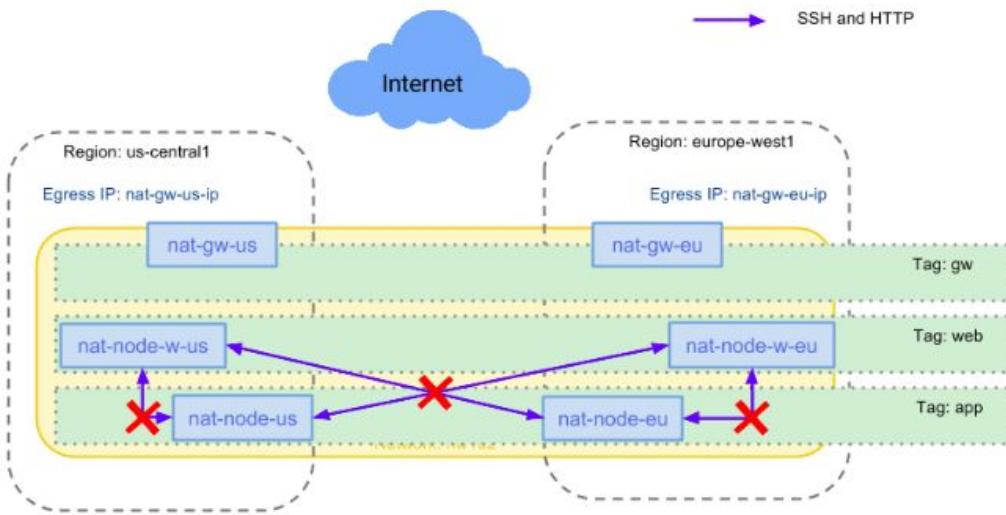
```
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute firewall-rules create nw102-allow-ssh --network nw102 --source-ranges 47.34.9.131 --allow tcp:22
Creating firewall...:Created [https://www.googleapis.com/compute/v1/projects/assignment1-230117/global/firewalls/nw102-allow-ssh].
Creating firewall...done.
NAME          NETWORK  DIRECTION  PRIORITY  ALLOW    DENY    DISABLED
nw102-allow-ssh  nw102    INGRESS     1000      tcp:22    False
```

## Creating a Tiered Network

This shows the architectural relations between the web servers and application servers.

According to the Networking 102 instruction, the subnetworks can be used as a complement to segmenting. Logical routing and firewalls are done by tags and not subnetworks





## Creating web servers

the procedure will show how to set up a web server in a virtual instance

```
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute instances create nat-node-w-us --network nw102 --subnet nw102-us --zone us-central1-f --image-family debian-9 --image-project debian-cloud --no-address --tags nat-us
Created [https://www.googleapis.com/compute/v1/projects/assignment1-230117/zones/us-central1-f/instances/nat-node-w-us].
NAME          ZONE          MACHINE_TYPE  PREEMPTIBLE  INTERNAL_IP  EXTERNAL_IP  STATUS
nat-node-w-us  us-central1-f  n1-standard-1      192.168.10.7    RUNNING
```

Compute Engine		VM instances	CREATE INSTANCE	IMPORT VM	REFRESH	START	STOP	RESET	DELETE																																				
VM Instances		<div style="display: flex; justify-content: space-between;"> <span>Filter VM instances</span> <span>Columns ▾</span> </div> <table border="1"> <thead> <tr> <th>Name</th> <th>Zone</th> <th>Recommendation</th> <th>Internal IP</th> <th>External IP</th> <th>Connect</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/> nat-gw-eu</td> <td>europe-west1-c</td> <td></td> <td>192.168.20.5 (nic0)</td> <td>35.240.114.41</td> <td>SSH ▾</td> </tr> <tr> <td><input checked="" type="checkbox"/> nat-gw-us</td> <td>us-central1-f</td> <td></td> <td>192.168.10.5 (nic0)</td> <td>35.193.130.109</td> <td>SSH ▾</td> </tr> <tr> <td><input checked="" type="checkbox"/> nat-node-eu</td> <td>europe-west1-c</td> <td></td> <td>192.168.20.6 (nic0)</td> <td>None</td> <td>SSH ▾</td> </tr> <tr> <td><input checked="" type="checkbox"/> nat-node-us</td> <td>us-central1-f</td> <td></td> <td>192.168.10.6 (nic0)</td> <td>None</td> <td>SSH ▾</td> </tr> <tr> <td><input checked="" type="checkbox"/> nat-node-w-us</td> <td>us-central1-f</td> <td></td> <td>192.168.10.7 (nic0)</td> <td>None</td> <td>SSH ▾</td> </tr> </tbody> </table>								Name	Zone	Recommendation	Internal IP	External IP	Connect	<input checked="" type="checkbox"/> nat-gw-eu	europe-west1-c		192.168.20.5 (nic0)	35.240.114.41	SSH ▾	<input checked="" type="checkbox"/> nat-gw-us	us-central1-f		192.168.10.5 (nic0)	35.193.130.109	SSH ▾	<input checked="" type="checkbox"/> nat-node-eu	europe-west1-c		192.168.20.6 (nic0)	None	SSH ▾	<input checked="" type="checkbox"/> nat-node-us	us-central1-f		192.168.10.6 (nic0)	None	SSH ▾	<input checked="" type="checkbox"/> nat-node-w-us	us-central1-f		192.168.10.7 (nic0)	None	SSH ▾
Name	Zone	Recommendation	Internal IP	External IP	Connect																																								
<input checked="" type="checkbox"/> nat-gw-eu	europe-west1-c		192.168.20.5 (nic0)	35.240.114.41	SSH ▾																																								
<input checked="" type="checkbox"/> nat-gw-us	us-central1-f		192.168.10.5 (nic0)	35.193.130.109	SSH ▾																																								
<input checked="" type="checkbox"/> nat-node-eu	europe-west1-c		192.168.20.6 (nic0)	None	SSH ▾																																								
<input checked="" type="checkbox"/> nat-node-us	us-central1-f		192.168.10.6 (nic0)	None	SSH ▾																																								
<input checked="" type="checkbox"/> nat-node-w-us	us-central1-f		192.168.10.7 (nic0)	None	SSH ▾																																								
Instance groups																																													
Instance templates																																													
Sole tenant nodes																																													
Disks																																													
Snapshots																																													
Images																																													

```
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute instances create nat-node-w-edu - -network nw102 --subnet nw102-eu --zone europe-west1-c --image-family centos-7 --image-project centos-cloud --no-address --tags nat-edu
Created [https://www.googleapis.com/compute/v1/projects/assignment1-230117/zones/europe-west1-c/instances/nat-node-w-edu].
NAME          ZONE          MACHINE_TYPE  PREEMPTIBLE  INTERNAL_IP  EXTERNAL_IP  STATUS
nat-node-w-edu  europe-west1-c  n1-standard-1      192.168.20.7    RUNNING
nouroudine@nouroudine-HP-PAVILION-Notebook:~$
```

The screenshot shows the Google Cloud Compute Engine interface. On the left, a sidebar menu includes options like VM instances, Instance groups, Instance templates, Sole tenant nodes, Disks, Snapshots, Images, and TPUs. The main area displays a table of VM instances with columns for Name, Zone, Recommendation, Internal IP, External IP, and Connect. The table lists six instances:

Name	Zone	Recommendation	Internal IP	External IP	Connect
nat-gw-eu	europe-west1-c		192.168.20.5 (nic0)	35.240.114.41	SSH
nat-gw-us	us-central1-f		192.168.10.5 (nic0)	35.193.130.109	SSH
nat-node-eu	europe-west1-c		192.168.20.6 (nic0)	None	SSH
nat-node-us	us-central1-f		192.168.10.6 (nic0)	None	SSH
nat-node-w-edu	europe-west1-c		192.168.20.7 (nic0)	None	SSH
nat-node-w-us	us-central1-f		192.168.10.7 (nic0)	None	SSH

## Apache servers installed and running

```
[nouroudine@nat-gw-eu ~]$ sudo service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
  Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)
  Active: active (running) since Wed 2019-01-30 22:19:26 UTC; 19s ago
    Docs: man:httpd(8)
          man:apachectl(8)
  Main PID: 22711 (httpd)
    Status: "Total requests: 0; Current requests/sec: 0; Current traffic: 0 B/sec"
   CGroup: /system.slice/httpd.service
           ├─22711 /usr/sbin/httpd -DFOREGROUND
           ├─22712 /usr/sbin/httpd -DFOREGROUND
           ├─22713 /usr/sbin/httpd -DFOREGROUND
           ├─22714 /usr/sbin/httpd -DFOREGROUND
           ├─22715 /usr/sbin/httpd -DFOREGROUND
           └─22716 /usr/sbin/httpd -DFOREGROUND

Jan 30 22:19:26 nat-gw-eu systemd[1]: Starting The Apache HTTP Server...
Jan 30 22:19:26 nat-gw-eu systemd[1]: Started The Apache HTTP Server.
[nouroudine@nat-gw-eu ~]$
```

```
nouroudine@nat-gw-us:~$ sudo service apache2 status
● apache2.service - The Apache HTTP Server
  Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
  Active: active (running) since Thu 2019-01-31 02:04:28 UTC; 1min 29s ago
  Main PID: 32323 (apache2)
   CGroup: /system.slice/apache2.service
           ├─32323 /usr/sbin/apache2 -k start
           ├─32325 /usr/sbin/apache2 -k start
           └─32326 /usr/sbin/apache2 -k start

Jan 31 02:04:27 nat-gw-us systemd[1]: Starting The Apache HTTP Server...
Jan 31 02:04:28 nat-gw-us systemd[1]: Started The Apache HTTP Server.
[nouroudine@nat-gw-us:~$ ]
```

## Partition network tiers with firewall rules

### Lockdown the network

```
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute firewall-rules create nw102-allow-internal --network nw102 --source-ranges 192.168.10.0/24,192.168.20.0/24 --allow tcp,udp,icmp
Creating firewall...:Created [https://www.googleapis.com/compute/v1/projects/assignment1-230117/global/firewalls/nw102-allow-internal].
NAME          NETWORK  DIRECTION  PRIORITY  ALLOW      DENY      DISABLED
nw102-allow-internal  nw102    INGRESS    1000     tcp,udp,icmp   False
nouroudine@nouroudine-HP-PAVILION-Notebook:~$
```

### Assign tags

```
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute instances add-tags nat-gw-us --zone us-central1-f --tags gw
Updated [https://www.googleapis.com/compute/v1/projects/assignment1-230117/zones/us-central1-f/instances/nat-gw-us].
nouroudine@nouroudine-HP-PAVILION-Notebook:~$
```

```
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute instances add-tags nat-gw-eu --zone europe-west1-c --tags gw
Updated [https://www.googleapis.com/compute/v1/projects/assignment1-230117/zones/europe-west1-c/instances/nat-gw-eu].
nouroudine@nouroudine-HP-PAVILION-Notebook:~$
```

```
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute instances add-tags nat-node-us --zone us-central1-f --tags app
Updated [https://www.googleapis.com/compute/v1/projects/assignment1-230117/zones/us-central1-f/instances/nat-node-us].
nouroudine@nouroudine-HP-PAVILION-Notebook:~$
```

```
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute instances add-tags nat-node-eu --zone europe-west1-c --tags app
Updated [https://www.googleapis.com/compute/v1/projects/assignment1-230117/zones/europe-west1-c/instances/nat-node-eu].
```

```
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute instances add-tags nat-node-w-us --zone us-central1-f --tags app
Updated [https://www.googleapis.com/compute/v1/projects/assignment1-230117/zones/us-central1-f/instances/nat-node-w-us].
nouroudine@nouroudine-HP-PAVILION-Notebook:~$
```

```
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute instances add-tags nat-node-w-us --zone us-central1-f --tags web
Updated [https://www.googleapis.com/compute/v1/projects/assignment1-230117/zones/us-central1-f/instances/nat-node-w-us].
```

Permit HTTP and SSH: Create additional firewall rules to permit curl among VMs in the same tier or for the NAT gateways.

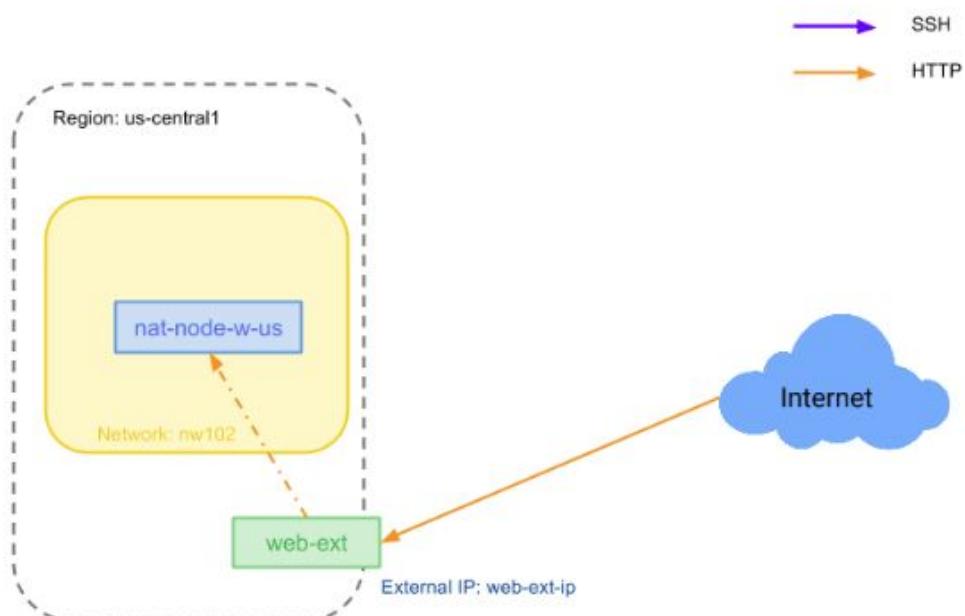
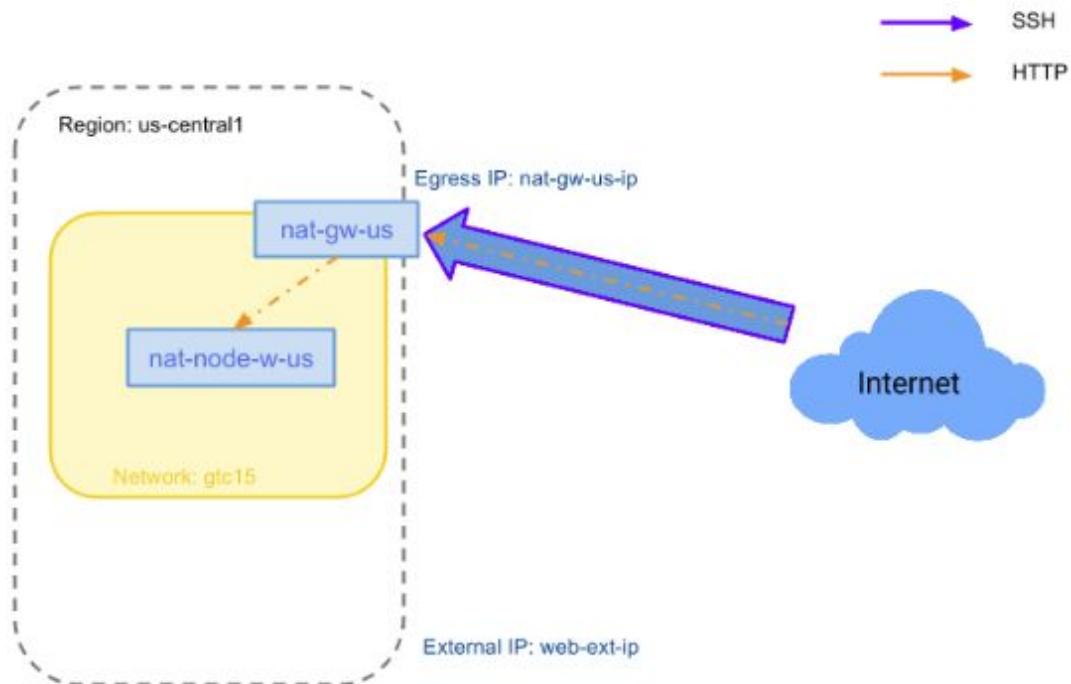
```
nw102-allow-ssh  nw102    INGRESS    1000    tcp:22,tcp:80    False
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute firewall-rules create nw102-allow-web --network nw102 --source-tags gw,web --target-tags web --allow tcp:22,tcp:80
Creating firewall...:Created [https://www.googleapis.com/compute/v1/projects/assignment1-230117/global/firewalls/nw102-allow-web].
```

```
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute firewall-rules create nw102-allow-app --network nw102 --source-tags gw,app --target-tags app --allow tcp:22,tcp:80  
Creating firewall...:Created [https://www.googleapis.com/compute/v1/projects/assignment1-230117/global/firewalls/nw102-allow-app].  
Creating firewall...done.  
NAME          NETWORK  DIRECTION  PRIORITY  ALLOW          DENY  DISABLED  
nw102-allow-app  nw102    INGRESS    1000     tcp:22,tcp:80      False  
nouroudine@nouroudine-HP-PAVILION-Notebook:~$
```

```
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute firewall-rules create nw102-allow-egress --network nw102 --source-tags app,web --target-tags gw --allow tcp:80,tcp:443  
Creating firewall...:Created [https://www.googleapis.com/compute/v1/projects/assignment1-230117/global/firewalls/nw102-allow-egress].  
Creating firewall...done.  
NAME          NETWORK  DIRECTION  PRIORITY  ALLOW          DENY  DISABLED  
nw102-allow-egress  nw102    INGRESS    1000     tcp:80,tcp:443      False  
nouroudine@nouroudine-HP-PAVILION-Notebook:~$
```

```
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute firewall-rules create nw102-allow-traceroute --network nw102 --source-ranges 192.168.10.0/24 --target-tags gw --allow udp:33434-33534  
Creating firewall...:Created [https://www.googleapis.com/compute/v1/projects/assignment1-230117/global/firewalls/nw102-allow-traceroute].  
Creating firewall...done.  
NAME          NETWORK  DIRECTION  PRIORITY  ALLOW          DENY  DISABLED  
nw102-allow-traceroute  nw102    INGRESS    1000     udp:33434-33534      False  
nouroudine@nouroudine-HP-PAVILION-Notebook:~$
```

## Alternate connectivity options



## Create forwarding rule to access internal resources

Add a new firewall to allow external access to web services in tier web

```
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute firewall-rules create nw102-allow-ext --network nw102 --source-ranges 0.0.0.0/0 --target-tags web --allow tcp:80
Creating firewall...:Created [https://www.googleapis.com/compute/v1/projects/assignment1-230117/global/firewalls/nw102-allow-ext].
Creating firewall...done.
NAME          NETWORK  DIRECTION  PRIORITY  ALLOW      DENY    DISABLED
nw102-allow-ext  nw102    INGRESS     1000      tcp:80    False
nouroudine@nouroudine-HP-PAVILION-Notebook:~$
```

Create the forwarding rule to expose web service through another external IP

```
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute addresses create web-ext-ip --region us-central1
Created [https://www.googleapis.com/compute/v1/projects/assignment1-230117/regions/us-central1/addresses/web-ext-ip].
nouroudine@nouroudine-HP-PAVILION-Notebook:~$
```

```
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute addresses create web-ext-ip --region us-central1
Created [https://www.googleapis.com/compute/v1/projects/assignment1-230117/regions/us-central1/addresses/web-ext-ip].
nouroudine@nouroudine-HP-PAVILION-Notebook:~$
```

```
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute target-instances create web-target --instance nat-node-w-us --zone us-central1-f
Created [https://www.googleapis.com/compute/v1/projects/assignment1-230117/zones/us-central1-f/targetInstances/web-target].
NAME   ZONE     INSTANCE   NAT_POLICY
web-target  us-central1-f  nat-node-w-us  NO_NAT
nouroudine@nouroudine-HP-PAVILION-Notebook:~$
```

```
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute forwarding-rules create web-ext -address web-ext-ip --port-range 80 --region us-central1 --target-instance web-target --target-instance-zone us-central1-f
WARNING: The --port-range flag is deprecated. Use equivalent --ports=80 flag.
Created [https://www.googleapis.com/compute/v1/projects/assignment1-230117/regions/us-central1/forwardingRules/web-ext].
nouroudine@nouroudine-HP-PAVILION-Notebook:~$
```

For some reason, it is impossible to install an apache server on nat-node-us and nat-node-eu.

Therefore, it is not possible to install a web content from the browser.

```
nouroudine@nat-node-us:~$ sudo apt install apache2
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libaprpri libaprutil1 libaprutil1-dbd-sqlite3
  libaprutil1-ldap libcurl57 liblua5.2-0 libperl5.24 libxml2 perl perl-modules-5.24 rename
  sgml-base ssl-cert xml-core
Suggested packages:
  www-browser apache2-doc apache2-suexec-pristine | apache2-suexec-custom perl-doc
  libterm-readline-gnu-perl | libterm-readline-perl-perl make sgml-base-doc
  openssl-blacklist debhelper
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute ssh nat-gw-eu --ssh-flag="-A" --zone europe-west1-c
Last login: Thu Jan 31 22:48:36 2019 from 47.34.9.131
[nouroudine@nat-gw-eu ~]$ ssh nat-node-eu
The authenticity of host 'nat-node-eu (192.168.20.3)' can't be established.
ECDSA key fingerprint is SHA256:x5vt2SnU0GnB8EHG2TmuMya8VPtcIleZs0/0zPwkL6M.
```

## Support server rotation and IP migration

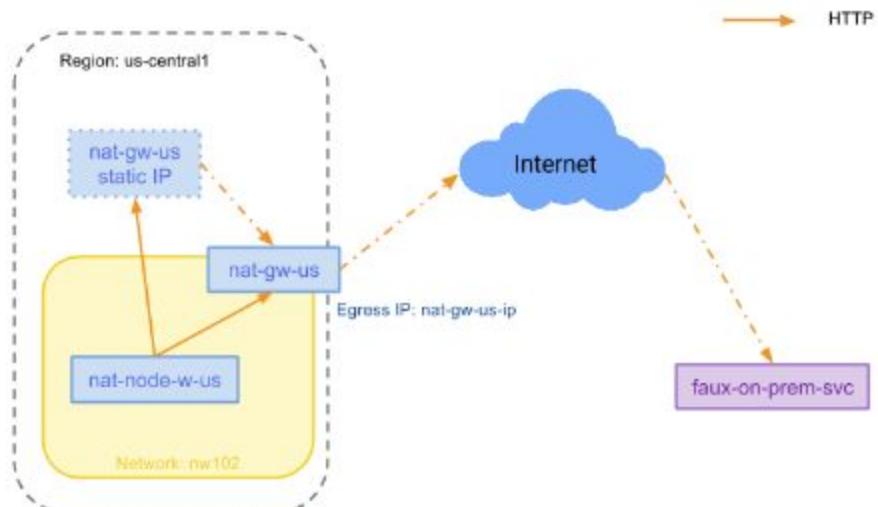
In preparation for the IP migration, create a new forwarding rule with a new IP address.

```
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute addresses create new-web-ext-ip --region europe-west1
Created [https://www.googleapis.com/compute/v1/projects/assignment1-230117/regions/europe-west1/addresses/new-web-ext-ip].
nouroudine@nouroudine-HP-PAVILION-Notebook:~$
```

```
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute target-instances create new-web-target --instance nat-node-w-eu --zone europe-west1-c
Created [https://www.googleapis.com/compute/v1/projects/assignment1-230117/zones/europe-west1-c/targetInstances/new-web-target].
NAME          ZONE      INSTANCE      NAT_POLICY
new-web-target europe-west1-c  nat-node-w-eu  NO_NAT
nouroudine@nouroudine-HP-PAVILION-Notebook:~$
```

```
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute forwarding-rules create new-web-ext --address new-web-ext-ip --port-range 80 --region europe-west1 --target-instance new-web-target --target-instance-zone europe-west1-c
WARNING: The --port-range flag is deprecated. Use equivalent --ports=80 flag.
Created [https://www.googleapis.com/compute/v1/projects/assignment1-230117/regions/europe-west1/forwardingRules/new-web-ext].
nouroudine@nouroudine-HP-PAVILION-Notebook:~$
```

## External Resource Mapping



## Map an external service through an internal IP

Create a standalone VM in the default network with web serving capability and create a firewall to allow traffic to it via TCP and port 80:

```
nouroutine@nouroutine-HP-PAVILION-Notebook:~$ gcloud compute instances create faux-on-perm-svc --network default --zone us-central1-f --image-family debian-9 --image-project debian-cloud --tags http-server  
Created [https://www.googleapis.com/compute/v1/projects/assignment1-230117/zones/us-central1-f/instances/faux-on-perm-svc].  
NAME          ZONE        MACHINE_TYPE  PREEMPTIBLE INTERNAL_IP  EXTERNAL_IP    STATUS  
faux-on-perm-svc  us-central1-f  n1-standard-1   10.128.0.2  35.184.237.112  RUNNING
```

```
nouroutine@nouroutine-HP-PAVILION-Notebook:~$ gcloud compute firewall-rules create default-allow-http-server --network default --target-tags http-server --allow tcp:80  
Creating firewall...[Created [https://www.googleapis.com/compute/v1/projects/assignment1-230117/global/firewalls/default-allow-http-server].  
Creating firewall...done.  
NAME          NETWORK  DIRECTION  PRIORITY  ALLOW  DENY  DISABLED  
default-allow-http-server  default  INGRESS  1000    tcp:80  False
```

Install Apache on the standalone VM that was just created

```
nouroudine@faux-on-perm-svc:~$ sudo service apache2 status
● apache2.service - The Apache HTTP Server
  Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
  Active: active (running) since Thu 2019-01-31 09:29:46 UTC; 17s ago
    Main PID: 1709 (apache2)
      CGroup: /system.slice/apache2.service
              ├─1709 /usr/sbin/apache2 -k start
              ├─1711 /usr/sbin/apache2 -k start
              └─1712 /usr/sbin/apache2 -k start

Jan 31 09:29:46 faux-on-perm-svc systemd[1]: Starting The Apache HTTP Server...
Jan 31 09:29:46 faux-on-perm-svc systemd[1]: Started The Apache HTTP Server.
```

Mapping of web service as internal service using iptables

```
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute firewall-rules create nw102-allow-on-prem --network nw102 --source-tags app,web --target-tags gw --allow tcp:80  
Creating firewall...:Created [https://www.googleapis.com/compute/v1/projects/assignment1-230117/global/firewalls/nw102-allow-on-prem].  
Creating firewall...done.  


| NAME                | NETWORK | DIRECTION | PRIORITY | ALLOW  | DENY | DISABLED |
|---------------------|---------|-----------|----------|--------|------|----------|
| nw102-allow-on-prem | nw102   | INGRESS   | 1000     | tcp:80 |      | False    |

  
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ █
```

# Configurations interfaces

Google Cloud Platform		Assignment1				
VPC network		External IP addresses		<a href="#">RESERVE STATIC ADDRESS</a>	<a href="#">REFRESH</a>	<a href="#">RELEASE STATIC ADDRESS</a>
<a href="#">VPC networks</a>						
<a href="#">External IP addresses</a>						
<a href="#">Firewall rules</a>						
<a href="#">Routes</a>						
<a href="#">VPC network peering</a>						
<a href="#">Shared VPC</a>						

VPC network		Firewall rules		<a href="#">CREATE FIREWALL RULE</a>	<a href="#">REFRESH</a>	<a href="#">DELETE</a>
VPC networks		Firewall rules		<a href="#">CREATE FIREWALL RULE</a>	<a href="#">REFRESH</a>	<a href="#">DELETE</a>
<a href="#">VPC networks</a>						
<a href="#">External IP addresses</a>						
<a href="#">Firewall rules</a>						
<a href="#">Routes</a>						
<a href="#">VPC network peering</a>						
<a href="#">Shared VPC</a>						

## Float static IP for mapped service

### Network interface configuration

```
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute routes create nw102-192-168-30-11
--network nw102 --destination-range 192.168.30.11/32 --next-hop-instance nat-gw-us --next-hop
--instance-zone us-central1-f
Created [https://www.googleapis.com/compute/v1/projects/assignment1-230321/global/routes/nw102-192-168-30-11].
NAME          NETWORK  DEST_RANGE           NEXT_HOP          PRIORITY
nw102-192-168-30-11  nw102   192.168.30.11/32  us-central1-f/instances/nat-gw-us  1000
nouroudine@nouroudine-HP-PAVILION-Notebook:~$
```

```

nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute firewall-rules create nw102-allow-on-prem-alt --network nw102 --source-ranges 192.168.0.0/19 --target-tags gw --allow tcp:80
Creating firewall...:Created [https://www.googleapis.com/compute/v1/projects/assignment1-230321/global/firewalls/nw102-allow-on-prem-alt].
Creating firewall...done.
NAME          NETWORK  DIRECTION  PRIORITY  ALLOW      DENY      DISABLED
nw102-allow-on-prem-alt  nw102    INGRESS    1000      tcp:80    False
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ █

```

The configuration is well done, but curl command failed to connect to the target:

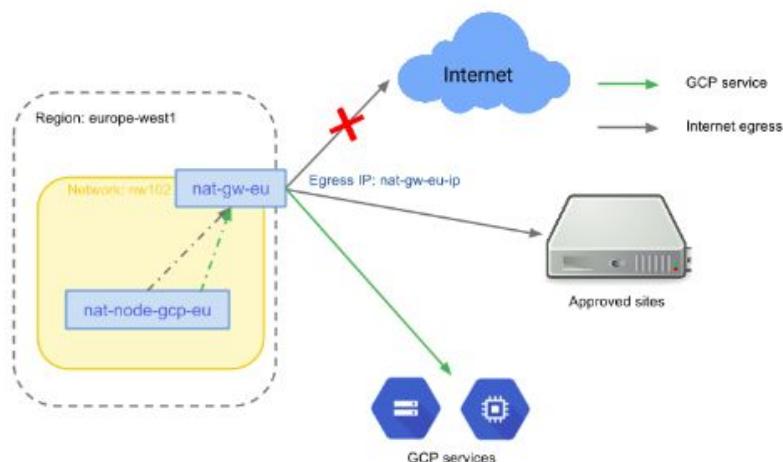
```

nouroudine@nat-node-us:~$ curl 192.168.30.11
curl: (7) Failed to connect to 192.168.30.11 port 80: Connection timed out
nouroudine@nat-node-us:~$ curl 192.168.30.11
curl: (7) Failed to connect to 192.168.30.11 port 80: Connection timed out
nouroudine@nat-node-us:~$ curl 192.168.30.11
curl: (7) Failed to connect to 192.168.30.11 port 80: Connection timed out
nouroudine@nat-node-us:~$ █

```

## Egress Proxy

Configurations of proxy using NAT gateway functionalities

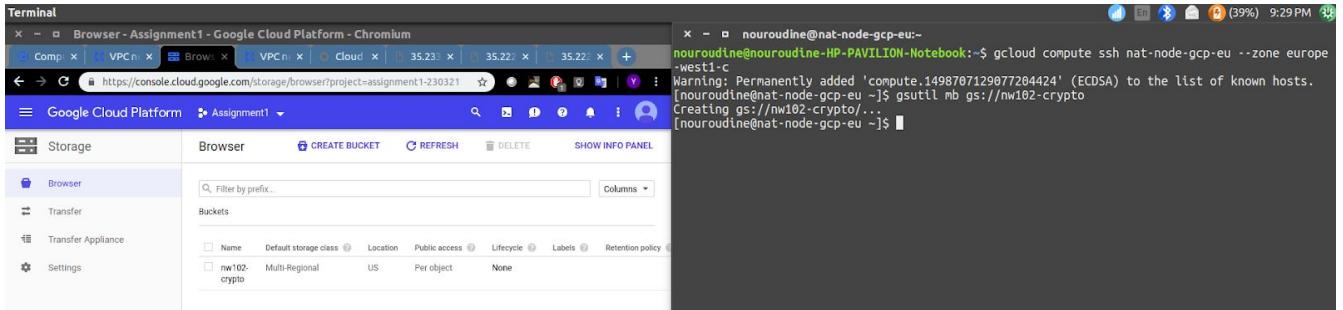


## Create new VM and verify default access

The following will show the different steps of the installation and configurations

```
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute instances create nat-node-gcp-eu --network nw102 --subnet nw102-eu --zone europe-west1-c --image-family centos-7 --image-project centos-cloud --scopes cloud-platform
Created [https://www.googleapis.com/compute/v1/projects/assignment1-230321/zones/europe-west1-c/instances/nat-node-gcp-eu].
NAME      ZONE      MACHINE_TYPE  PREEMPTIBLE INTERNAL_IP  EXTERNAL_IP   STATUS
nat-node-gcp-eu  europe-west1-c  n1-standard-1          192.168.20.5  184.155.93.227  RUNNING
nouroudine@nouroudine-HP-PAVILION-Notebook:~$
```

Bucket created:



Curl worked like a charm

```
[nouroudine@nat-node-gcp-eu ~]$ curl -L www.google.com
<!DOCTYPE html>html.itemscope="" itemtype="http://schema.org/WebPage" lang="en"><head><meta content="Search the world's information, including webpages, images, videos and more. Google has many special features to help you find exactly what you're looking for." name="description"><meta content="noodp" name="robots"><meta content="text/html; charset=UTF-8" http-equiv="Content-Type" /><meta content="/images/branding/goolge/leg/1x/googleleg_standard_color_128dp.png" itemprop="image"/><title>Google</title><script nonce="47755zwtV0X4zRols2Dyg==">(function(){window.google=(kE I:'S7STXK7dEcQyA7yJrp4B',kEXPT:'0,1353747,57,1957,1817,1406,598,527,730,1458,115,234,30,695,533,885,18,71,253,841,132,2334979,329520,1294,12383,4855,32692,15247,867,18761,1696,4987,1180,3335,1,2,4669,2192,369,1161,7,2147,5505,224,1817,1195,266,4294,983,575,833,284,2,1386,2431,59,2,1,3,1297,284,3586,453,3390,16,308,1267,774,2254,1403,3337,1146,5,2,2,1986,2593,182,283,3134,669,1058,1889,1129,268,183,7,1,2,3,463,620,29,983,6,466,458,1847,769,536,695,3395,1289,792,84,412,2,554,2635,389,438,516,280,1226,401,557,270,448,155,37,1186,1296,68,484,47,1889,1284,424,1928,798,8,2,259,499,2145,265,2,366,265,217,942,1403,2,4,2,149,530,44,165,169,36,564,8,828,417,187,162,167,82,98,149,1759,369,95,2190,17,12,620,464,694,256,44,227,79,25,330,110,294,360,21,317,255,2,8,3,340,597,1,394,357,983,695,228,186,183,11,287,327,38,372,518,3,314,417,32,298,214,2,396,36,42,348,30,398,233,98,13,248,85,332,358,5963777,2554,233,21,597582,2799958,4,1572,549,333,444,1,2,88,1,906,17,385,2,6,2,212,3,1,1,1,1,1,414,1,748,926,3,570,1,2,456,32,56,6,1,14,4,1,19,12,1,10,223656524',authUser=0,kssc:'c9c918f8e5757WK7dEcQyA7yJrp4B',ktl:'US');google.khl='en';})();a=a.parentNode;return b||google.getLEI=function(a){for(var b=a;ba.getAttribute('!');(b=b.getAttribute('eid')));}a=a.parentNode;return b;google.https=function(){return 'https://'+window.location.protocol};google.ml=function(){return null};google.loa=function(a,b,e,c,g){var d="";f=google.ls||"";e||-1!=b.search("§el=")||((d="§el=")+google.getEI(c),-1==b.search("§chid=")||((d="§chid=")+a.search("§chid=")));g||(d="§chid=")+a.search("§chid="));c="";!e&&(c=google.getEI(c))&&(d="§el=")!&&(c="§chid=")+a.search("§chid=");a=e||"/"+g||"gen 204")+"?atyp=i&ct="+a}}();google.vel&google.vel.lu&google.vel.lu="a";b.src=a.google.li=f+1);google.logUrl=function(a,b,e,c,g){var d="";f=google.ls||"";e||-1!=b.search("§el=")||((d="§el=")+google.getEI(c),-1==b.search("§chid=")||((d="§chid=")+a.search("§chid=")));c="";!e&&(c=google.getEI(c))&&(d="§el=")!&&(c="§chid=")+a.search("§chid="));a=e||"/"+g||"gen 204")+"?atyp=i&ct="+a}}();
```

```
[nouroudine@nat-node-gcp-eu ~]$ curl -L www.iana.org
<!DOCTYPE html>
<html>
<head>
    <title>Internet Assigned Numbers Authority</title>
    <meta charset="utf-8" />
    <meta http-equiv="Content-type" content="text/html; charset=utf-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1" />
    <link rel="stylesheet" media="screen" href="/_css/2015.1/screen.css"/>
    <link rel="stylesheet" media="print" href="/_css/2015.1/print.css"/>
    <link rel="shortcut icon" type="image/ico" href="/_img/bookmark_icon.ico"/>
    <script type="text/javascript" src="/_js/2013.1/jquery.js"></script>
    <script type="text/javascript" src="/_js/2013.1/iana.js"></script>
```

```
[nouroudine@nat-node-gcp-eu ~]$ curl 35.222.233.0
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
    <head>
        <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
        <title>Apache2 Debian Default Page: It works</title>
        <style type="text/css" media="screen">
        *
        {
            margin: 0px 0px 0px 0px;
            padding: 0px 0px 0px 0px;
        }
        body, html {
            padding: 3px 3px 3px 3px;
        }
    </style>
</head>
<body>
    It works!
</body>
</html>
```

Trying to access Google Cloud platform resources: The request is not working as they might be suspected

```
[nouroudine@nat-node-gcp-eu ~]$ gsutil ls gs://
INFO 0201 04:11:36.581570 retry_util.py] Retrying request, attempt #1...
INFO 0201 04:12:38.820609 retry_util.py] Retrying request, attempt #2...
INFO 0201 04:13:42.331372 retry_util.py] Retrying request, attempt #3...
INFO 0201 04:14:49.447334 retry_util.py] Retrying request, attempt #4...
INFO 0201 04:16:03.328412 retry_util.py] Retrying request, attempt #5...
```

## Deploy a proxy service for limited access

The installation of Squid is required for the configuration of an egress whitelist to include googleapis.com

```
[nouroudine@nat-gw-eu ~]$ yum install squid -y
Loaded plugins: fastestmirror
You need to be root to perform this command.
[nouroudine@nat-gw-eu ~]$ sudo yum install squid -y
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: mirrors.sonic.net
 * epel: d2lzk7pfhq30w.cloudfront.net
 * extras: mirror.fileplanet.com
 * updates: mirror.fileplanet.com
Resolving Dependencies
--> Running transaction check
--> Package squid.x86_64 7:3.5.20-12.el7 will be installed
--> Processing Dependency: squid-migration-script for package: 7:squid-3.5.20-12.el7.x86_64
--> Processing Dependency: perl(Digest::MD5) for package: 7:squid-3.5.20-12.el7.x86_64
--> Processing Dependency: perl(Data::Dumper) for package: 7:squid-3.5.20-12.el7.x86_64
--> Processing Dependency: perl(DBI) for package: 7:squid-3.5.20-12.el7.x86_64
--> Processing Dependency: libltdl.so.7()(64bit) for package: 7:squid-3.5.20-12.el7.x86_64
--> Processing Dependency: libcap.so.3()(64bit) for package: 7:squid-3.5.20-12.el7.x86_64
--> Running transaction check
--> Package libcap.x86_64 0:1.0.0-1.el7 will be installed
--> Package libtool-ltdl.x86_64 0:2.4.2-22.el7_3 will be installed
--> Package perl-DBI.x86_64 0:1.627-4.el7 will be installed
--> Processing Dependency: perl(RPC::PlServer) >= 0.2001 for package: perl-DBI-1.627-4.el7.x86_64
--> Processing Dependency: perl(RPC::PlClient) >= 0.2000 for package: perl-DBI-1.627-4.el7.x86_64
--> Package perl-Daemon-Dumper.x86_64 0:2.145-3.el7 will be installed
--> Package perl-Digest-MD5.x86_64 0:2.52-3.el7 will be installed
--> Processing Dependency: perl(Digest::base) >= 1.00 for package: perl-Digest-MD5-2.52-3.el7.x86_64
--> Package squid-migration-script.x86_64 7:3.5.20-12.el7 will be installed
--> Running transaction check
--> Package perl-Digest.noarch 0:1.17-245.el7 will be installed
--> Package perl-PlRPC.noarch 0:0.2020-14.el7 will be installed
--> Processing Dependency: perl(Net::Daemon) >= 0.13 for package: perl-PlRPC-0.2020-14.el7.noarch
--> Processing Dependency: perl(Net::Daemon::Test) for package: perl-PlRPC-0.2020-14.el7.noarch
--> Processing Dependency: perl(Net::Daemon::Log) for package: perl-PlRPC-0.2020-14.el7.noarch
--> Processing Dependency: perl(Compress::Zlib) for package: perl-PlRPC-0.2020-14.el7.noarch
--> Running transaction check
--> Package perl-IO-Compress.noarch 0:2.061-2.el7 will be installed
--> Processing Dependency: perl(Compress::Raw::Zlib) >= 2.061 for package: perl-IO-Compress-2.061-2.el7.noarch
--> Processing Dependency: perl(Compress::Raw::Bzip2) >= 2.061 for package: perl-IO-Compress-2.061-2.el7.noarch
--> Package perl-Net-Daemon.noarch 0:0.48-5.el7 will be installed
--> Running transaction check
--> Package perl-Compress-Raw-Bzip2.x86_64 0:2.061-3.el7 will be installed
--> Package perl-Compress-Raw-Zlib.x86_64 1:2.061-4.el7 will be installed
--> Finished Dependency Resolution
```

```

Total                                         2.2 MB/s | 4.5 MB  00:00:02
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : perl-Data-Dumper-2.145-3.el7.x86_64          1/13
  Installing : perl-Net-Daemon-0.48-5.el7.noarch            2/13
  Installing : perl-Digest-1.17-245.el7.noarch            3/13
  Installing : perl-Digest-MD5-2.52-3.el7.x86_64          4/13
  Installing : 7:squid-migration-script-3.5.20-12.el7.x86_64 5/13
  Installing : 1:perl-Compress-Raw-Zlib-2.061-4.el7.x86_64 6/13
  Installing : libtool-ltdl-2.4.2-22.el7_3.x86_64          7/13
  Installing : libecap-1.0.0-1.el7.x86_64                  8/13
  Installing : perl-Compress-Raw-Bzip2-2.061-3.el7.x86_64 9/13
  Installing : perl-IO-Compress-2.061-2.el7.noarch        10/13
  Installing : perl-PlRPC-0.2020-14.el7.noarch           11/13
  Installing : perl-DBI-1.627-4.el7.x86_64              12/13
  Installing : 7:squid-3.5.20-12.el7.x86_64             13/13
  Verifying   : perl-Compress-Raw-Bzip2-2.061-3.el7.x86_64 1/13
  Verifying   : 7:squid-3.5.20-12.el7.x86_64             2/13
  Verifying   : perl-Data-Dumper-2.145-3.el7.x86_64          3/13
  Verifying   : perl-Digest-MD5-2.52-3.el7.x86_64          4/13
  Verifying   : libecap-1.0.0-1.el7.x86_64                  5/13
  Verifying   : perl-IO-Compress-2.061-2.el7.noarch        6/13
  Verifying   : libtool-ltdl-2.4.2-22.el7_3.x86_64          7/13
  Verifying   : 1:perl-Compress-Raw-Zlib-2.061-4.el7.x86_64 8/13
  Verifying   : 7:squid-migration-script-3.5.20-12.el7.x86_64 9/13
  Verifying   : perl-Digest-1.17-245.el7.noarch           10/13
  Verifying   : perl-DBI-1.627-4.el7.x86_64              11/13
  Verifying   : perl-Net-Daemon-0.48-5.el7.noarch        12/13
  Verifying   : perl-PlRPC-0.2020-14.el7.noarch           13/13

Installed:
  squid.x86_64 7:3.5.20-12.el7

Dependency Installed:
  libecap.x86_64 0:1.0.0-1.el7                      libtool-ltdl.x86_64 0:2.4.2-22.el7_3
  perl-Compress-Raw-Bzip2.x86_64 0:2.061-3.el7      perl-Compress-Raw-Zlib.x86_64 1:2.061-4.el7
  perl-DBI.x86_64 0:1.627-4.el7                    perl-Data-Dumper.x86_64 0:2.145-3.el7
  perl-Digest.noarch 0:1.17-245.el7                 perl-Digest-MD5.x86_64 0:2.52-3.el7
  perl-IO-Compress.noarch 0:2.061-2.el7            perl-Net-Daemon.noarch 0:0.48-5.el7
  perl-PlRPC.noarch 0:0.2020-14.el7                squid-migration-script.x86_64 7:3.5.20-12.el7

Complete!
[nouroudine@nat-gw-eu ~]$ 
[nouroudine@nat-gw-eu ~]$ sudo su -
[root@nat-gw-eu ~]# ca
```

## Squid is running

```

[nouroudine@nat-gw-eu ~]$ sudo service squid restart
Redirecting to /bin/systemctl restart squid.service
[nouroudine@nat-gw-eu ~]$ sudo service squid status
Redirecting to /bin/systemctl status squid.service
● squid.service - Squid caching proxy
   Loaded: loaded (/usr/lib/systemd/system/squid.service; disabled; vendor preset: disabled)
   Active: active (running) since Fri 2019-02-01 04:34:08 UTC; 19s ago
     Process: 13363 ExecStart=/usr/sbin/squid $SQUID_OPTS -f $SQUID_CONF (code=exited, status=0/SUCCESS)
    Main PID: 13365 (squid)
       CGroup: /system.slice/squid.service
               └─13365 /usr/sbin/squid -f /etc/squid/squid.conf
                  ├─13367 (squid-1) -f /etc/squid/squid.conf
                  ├─13368 (logfile-daemon) /var/log/squid/access.log

Feb 01 04:34:08 nat-gw-eu systemd[1]: Starting Squid caching proxy...
Feb 01 04:34:08 nat-gw-eu systemd[1]: Started Squid caching proxy.
Feb 01 04:34:08 nat-gw-eu squid[13365]: Squid Parent: will start 1 kids
Feb 01 04:34:08 nat-gw-eu squid[13365]: Squid Parent: (squid-1) process 13367 started
[nouroudine@nat-gw-eu ~]$ 
```

## Firewall configuration

```
nouroudine@nouroudine-HP-PAVILION-Notebook:~$ gcloud compute firewall-rules create nw102-allow-proxy --network nw102 --source-ranges 192.168.20.0/24 --target-tags gw --allow tcp:3128
Creating firewall...:Created [https://www.googleapis.com/compute/v1/projects/assignment1-230321/global/firewalls/nw102-allow-proxy].
Creating firewall...done.
+-----+
| NAME      NETWORK  DIRECTION  PRIORITY  ALLOW      DENY    DISABLED |
| nw102-allow-proxy  nw102     INGRESS    1000     tcp:3128   False   |
+-----+
nouroudine@nouroudine-HP-PAVILION-Notebook:~$
```

Testing the configuration with curl and it is working like a charm.

```
[nouroudine@nat-node-gcp-eu ~]$ curl 35.222.233.0
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
    <title>Apache2 Debian Default Page: It works</title>
    <style type="text/css" media="screen">
        *
        {
            margin: 0px 0px 0px 0px;
            padding: 0px 0px 0px 0px;
        }

        body, html {
            padding: 3px 3px 3px 3px;
            background-color: #08DBE2;

            font-family: Verdana, sans-serif;
            font-size: 11pt;
            text-align: center;
        }

        div.main_page {
            position: relative;
            display: table;
            width: 800px;
            margin-bottom: 3px;
            margin-left: auto;
            margin-right: auto;
            padding: 0px 0px 0px 0px;

            border-width: 2px;
            border-color: #212738;
            border-style: solid;
            background-color: #FFFFFF;
            text-align: center;
        }

        div.page_header {
            height: 99px;
            width: 100%;
        }
    </style>
</head>
<body>
    <div>
        <div>
            <h1>It works</h1>
            <p>This is the default web page for this server.<br/>
            The web server software is running normally.<br/>
            If you reached this page, your browser is working correctly.<br/>
            You can now close this window or tab, and return to your normal browsing activities.</p>
        </div>
    </div>
</body>
</html>
```

Testing the configuration by accessing Google resources and it works perfectly:

```
[nouroudine@nat-node-gcp-eu ~]$
[nouroudine@nat-node-gcp-eu ~]$ gsutil ls gs://
gs://nw102-crypto/
[nouroudine@nat-node-gcp-eu ~]$ █
```

```
[root@nat-node-gcp-eu ~]# cat <<EOF >>/etc/profile
> export no_proxy=".internal,localhost,127.0.0.1,metadata,169.254.169.254"
> EOF
[root@nat-node-gcp-eu ~]# exit
[output]
[nouroudine@nat-node-gcp-eu ~]$ exit
Logout
Connection to nat-node-gcp-eu closed.
[nouroudine@nat-gw-eu ~]$ ssh nat-node-gcp-eu
Last login: Fri Feb 1 04:43:43 2019 from nat-gw-eu.europe-west1-c.c.assignment1-230321.internal
[nouroudine@nat-node-gcp-eu ~]$ gcloud compute instances list
NAME          ZONE      MACHINE_TYPE PREEMPTIBLE INTERNAL_IP   EXTERNAL_IP     STATUS
nat-gw-eu     europe-west1-c n1-standard-1    192.168.20.2   35.233.55.219  RUNNING
nat-node-eu   europe-west1-c n1-standard-1    192.168.20.3   35.233.55.220  RUNNING
nat-node-gcp-eu europe-west1-c n1-standard-1    192.168.20.5   35.233.55.221  RUNNING
nat-node-w-eu europe-west1-c n1-standard-1    192.168.20.4   35.233.55.222  RUNNING
faux-on-prem-svc us-central1-f n1-standard-1    10.128.0.2     35.222.233.0   RUNNING
nat-gw-us     us-central1-f n1-standard-1    192.168.10.2    35.224.197.215  RUNNING
nat-node-us   us-central1-f n1-standard-1    192.168.10.3    35.184.253.14   RUNNING
```

