

IMPLEMENTATION OF AWS VPC ARTICTURE -- FULL SETUP

Overview

This Aws vpc articture presents the full setup of vpc including its major tools and configuration as default and other advance stuff are done manually. The below Articture is referenced from Aws official articture. I have mentioned all the points and steps that are done to set up this beginner level configuration and all the figures corresponding to the steps. And the important things that are not mentioned in blow steps are:

1.Security rules in every step:

i.Internetgateway firewalls

ii. subnet level security (NACL)

iii. Security groups on instance level

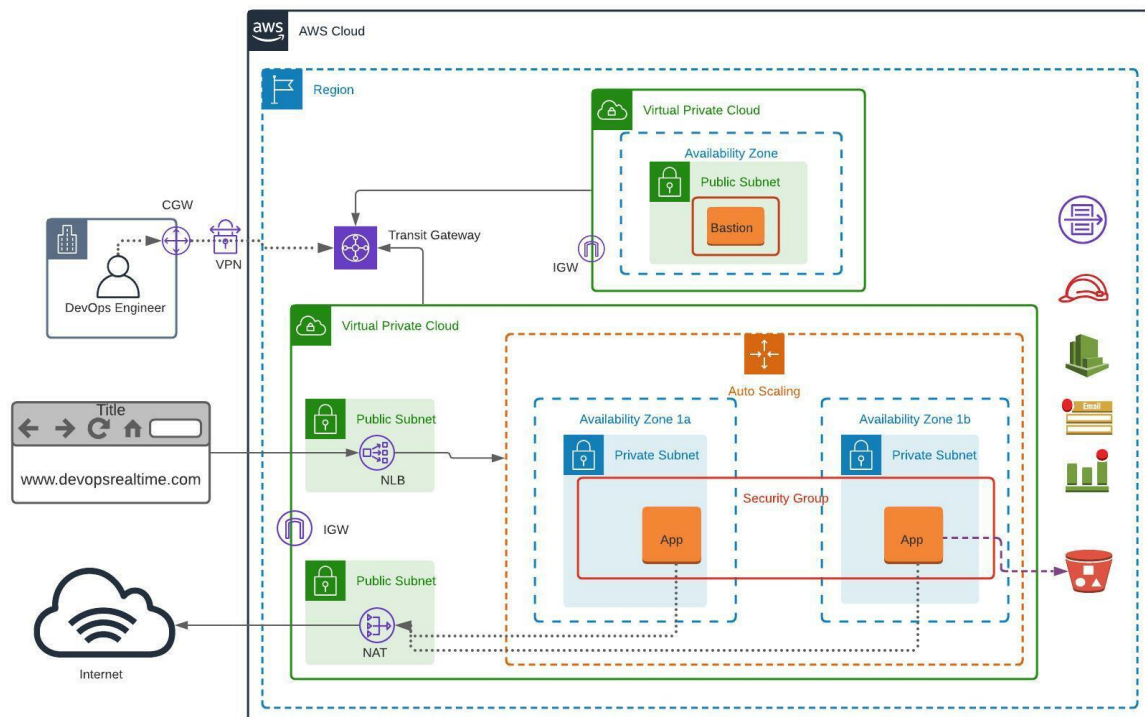
2.Other Kind of IDS and IPS

3.Route 53

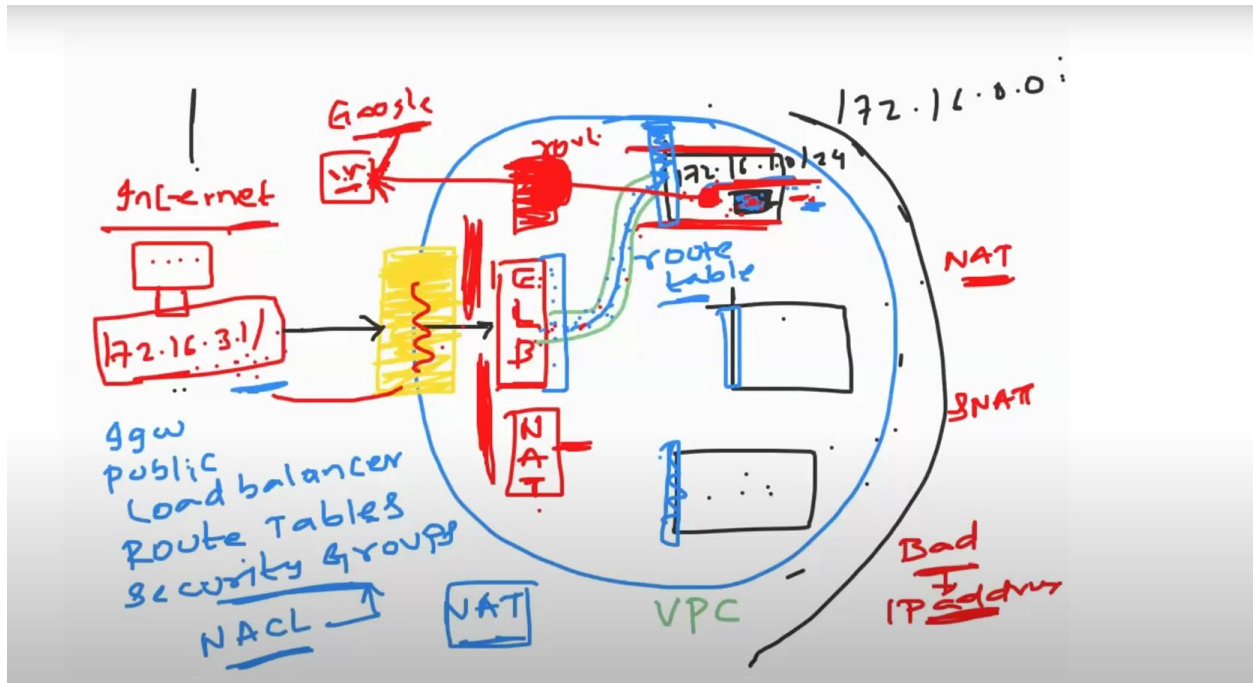
As I haven't implemented the route 53 in this basic Bigner level project, if any kind of DNS stuff, traffic flow, hosting's are basically handled by route53

Official Figure:

Anyone can take below diagram for reference which is also related with below steps that i have mentioned to create the vpc set up



My Draft Figure:



This is just a draft architecture of AWS VPC SIMPLE SETUP that I use to make the setup from scratch.

Some keys things done to setup aws vpc recommended articture


-Firstly, I just created a VPC on aws using my root user password, which is for my personal experiments, when creating vpc the most important things to configure are subnets and routing table to connect public subnets to Internetgateway and private subnets to interact to public subnets and NAT



-After that just created the autoscaling group integrated with ec2 instances that can be auto scalable with it is needed, that should be configured by knowing requirements in my case, base -2 and min -1, max-4 and that auto scaling group should be inside the private subnets to keep the server (EC2) integrated with it to be safe

Group details

Edit

Auto Scaling group name myscalinggroup	<div>Desired capacity</div> 2	<div>Desired capacity type</div> Units (number of instances)	<div>Amazon Resource Name (ARN)</div> <div> arn:aws:autoscaling:ap-southeast-2:339712713104:autoScalingGroup:c1451103-ad04-47ad-a575-f49557af417a:autoScalingGroupName/myscalinggroup</div>
<div>Date created</div> Sun Sep 29 2024 23:06:51 GMT+1000 (Australian Eastern Standard Time)	<div>Minimum capacity</div> 1	<div>Status</div> -	
	<div>Maximum capacity</div> 4		

Network

Edit

<div>Availability Zones</div> ap-southeast-2b, ap-southeast-2a	<div>Subnet ID</div> subnet-0bb66b320e467d21e, subnet-0ec235ae53e47ac7e	
--	---	--

-As the private subnet cannot connect with the internet, it should need a safe connection to give response to clients on behalf of the application inside that server. So, to connect with EC2 we need to create the server called BASTION in public subnet and we need to login to that bastion server which can be used to access the private server from that public bastion server.

Instance summary for i-0b71d187c0710fd56 (AWS_BASTAION) Info		
Updated less than a minute ago		
Refresh Connect Instance state ▼ Actions ▼		
Instance ID i-0b71d187c0710fd56 (AWS_BASTAION)	Public IPv4 address 54.252.145.114 open address	Private IPv4 addresses 10.0.16.91
IPv6 address -	Instance state Running	Public IPv4 DNS ec2-54-252-145-114.ap-southeast-2.compute.amazonaws.com open address
Hostname type IP name: ip-10-0-16-91.ap-southeast-2.compute.internal	Private IP DNS name (IPv4 only) ip-10-0-16-91.ap-southeast-2.compute.internal	Elastic IP addresses -
Answer private resource DNS name -	Instance type t2.micro	AWS Compute Optimizer finding Opt-in to AWS Compute Optimizer for recommendations. Learn more
Auto-assigned IP address 54.252.145.114 [Public IP]	VPC ID vpc-04214965e50b2466f (First-Project-vpc)	Auto Scaling Group name -
IAM Role -	Subnet ID subnet-02ac3d7e562c1ce49 (First-Project-subnet-public2-ap-southeast-2b)	
IMDSv2 Required	Instance ARN arn:aws:ec2:ap-southeast-2:339712713104:instance/i-0b71d187c0710fd56	

-I got access from public bastion server to private server using ssh by specifying the private key with its public key and i run server of python on port 8000 on both server by using giving different instruction and this is just done to check the load balancer working mechanism which is done in upcoming steps

```

ubuntu@ip-10-0-16-91:~$ ssh -i bastion-login.pem ubuntu@10.0.158.225
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.0-1012-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of Tue Oct  1 05:40:00 UTC 2024

System load:  0.0                Processes:            105
Usage of /:   29.4% of 6.71GB    Users logged in:     0
Memory usage: 25%                IPv4 address for enX0: 10.0.158.225
Swap usage:   0%

 * Ubuntu Pro delivers the most comprehensive open source security and
   compliance features.

   https://ubuntu.com/aws/pro

Expanded Security Maintenance for Applications is not enabled.

103 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

*** System restart required ***
Last login: Mon Sep 30 03:00:50 2024 from 10.0.16.91
ubuntu@ip-10-0-158-225:~$ ls
index.html
ubuntu@ip-10-0-158-225:~$ cat index.html
<!DOCTYPE html>
<html>
<body>

<h1>My First Heading</h1>
<p>My first paragraph.</p>

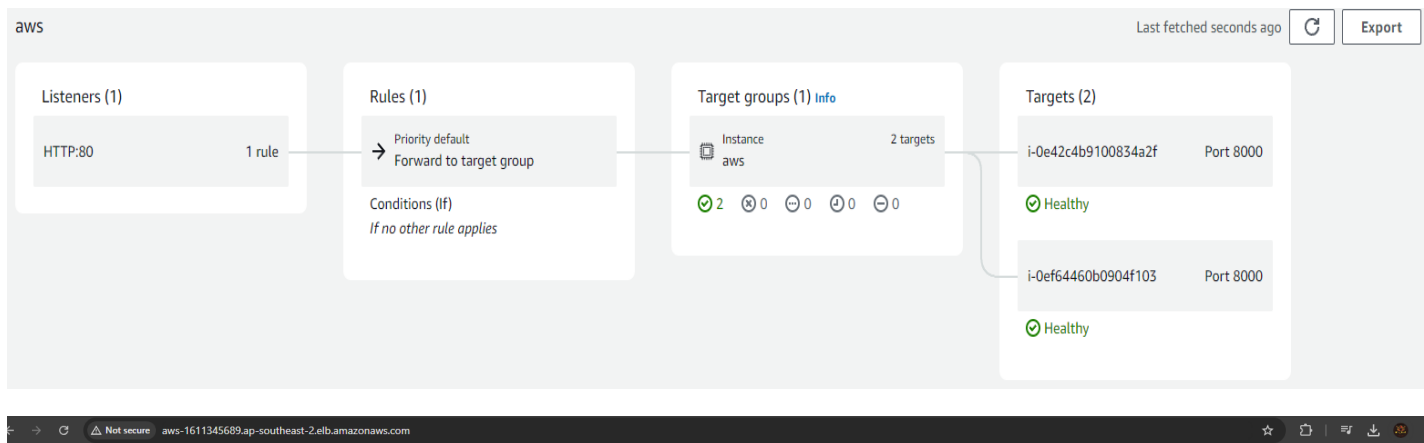
</body>
</html>
ubuntu@ip-10-0-158-225:~$ python3 -m http.server 8000

```

For private server 10.0.158.225- just written first heading, first paragraph

For private server 10.0.135.31 - just written second heading, second paragraph

-After those steps, I created a Load balancer that helps to balance the loads between different servers (ec2) and forwards the traffic from InterGate way to private servers.



second server is on now

```
ubuntu@ip-10-0-158-225: ~  
Swap usage: 0%  
  
* Ubuntu Pro delivers the most comprehensive open source security and  
compliance features.  
  
https://ubuntu.com/aws/pro  
  
Expanded Security Maintenance for Applications is not enabled.  
  
103 updates can be applied immediately.  
To see these additional updates run: apt list --upgradable  
  
Enable ESM Apps to receive additional future security updates.  
See https://ubuntu.com/esm or run: sudo pro status  
  
*** System restart required ***  
Last login: Tue Oct 1 05:40:01 2024 from 10.0.16.91  
ubuntu@ip-10-0-158-225:~$ ls  
index.html  
ubuntu@ip-10-0-158-225:~$ python3 -m http.server 8000  
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...  
10.0.22.117 - - [01/Oct/2024 06:52:00] "GET / HTTP/1.1" 200 -  
10.0.10.223 - - [01/Oct/2024 06:52:07] "GET / HTTP/1.1" 200 -  
10.0.22.117 - - [01/Oct/2024 06:52:30] "GET / HTTP/1.1" 200 -  
10.0.10.223 - - [01/Oct/2024 06:52:37] "GET / HTTP/1.1" 200 -  
10.0.22.117 - - [01/Oct/2024 06:53:00] "GET / HTTP/1.1" 200 -  
10.0.10.223 - - [01/Oct/2024 06:53:07] "GET / HTTP/1.1" 200 -  
10.0.22.117 - - [01/Oct/2024 06:53:30] "GET / HTTP/1.1" 200 -  
10.0.10.223 - - [01/Oct/2024 06:53:37] "GET / HTTP/1.1" 200 -
```

```
ubuntu@ip-10-0-135-31: ~  
105 updates can be applied immediately.  
To see these additional updates run: apt list --upgradable  
  
Enable ESM Apps to receive additional future security updates.  
See https://ubuntu.com/esm or run: sudo pro status  
  
*** System restart required ***  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
To run a command as administrator (user "root"), use "sudo <command>".  
See "man sudo_root" for details.  
ubuntu@ip-10-0-135-31:~$ vim index.html  
ubuntu@ip-10-0-135-31:~$ ls  
index.html  
ubuntu@ip-10-0-135-31:~$ python3 -m http.server 8000  
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...  
10.0.10.223 - - [01/Oct/2024 06:45:37] "GET / HTTP/1.1" 200 -  
10.0.22.117 - - [01/Oct/2024 06:45:43] "GET / HTTP/1.1" 200 -  
10.0.22.117 - - [01/Oct/2024 06:45:45] "GET / HTTP/1.1" 200 -  
10.0.22.117 - - [01/Oct/2024 06:45:46] "GET / HTTP/1.1" 200 -  
10.0.22.117 - - [01/Oct/2024 06:45:55] "GET / HTTP/1.1" 200 -  
10.0.22.117 - - [01/Oct/2024 06:45:56] "GET / HTTP/1.1" 200 -
```