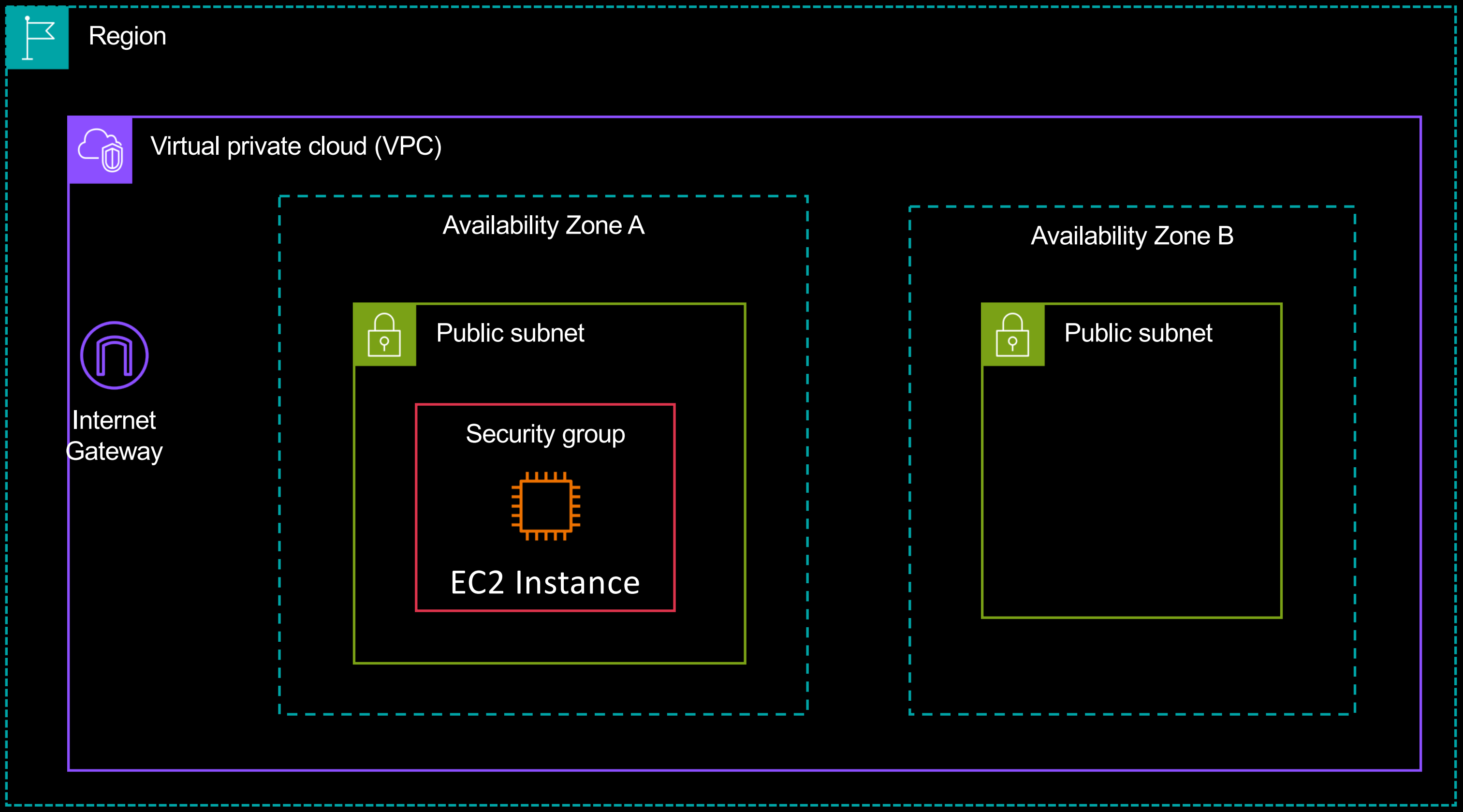
AWS Solution Architect Training

Module 02
Virtual Private Cloud (VPC)

Instructor: Tim Platt, Cloud Solution Architect

What we’ve just accomplished in our AWS Account


Region

Virtual private cloud (VPC)

Availability Zone A

Public subnet

Security group

EC2 Instance

Availability Zone B

Public subnet

Internet Gateway

Virtual Private Cloud (VPC)

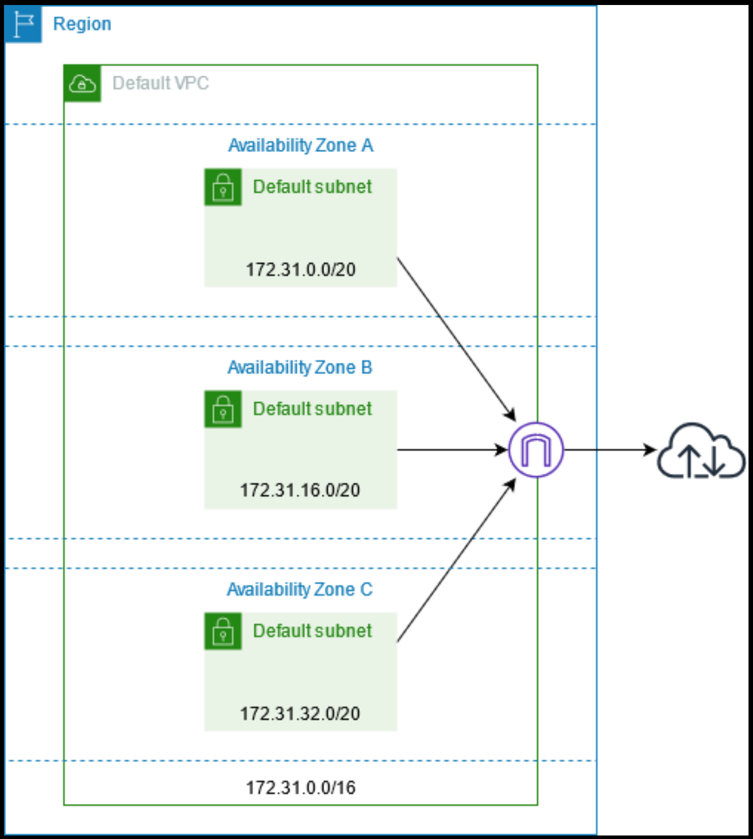
Network

A virtual network for your virtual servers in the cloud

Key Points

- A logically isolated section of the cloud where you can launch AWS resources
- Proper network design dictates having a layered or tiered network with “Defense in Depth” applying network level access controls
- Key sub-components:
  - Subnets (Public & Private)
  - Internet Gateway (IGW)
  - NAT Gateway (Network Address Translation)
  - Route Table entries for the virtual router
  - Firewall rules – Network Access Control Lists (ACLs) and Security Groups
- SUPERPOWER: Virtual equivalents of all the components needed to build a computer network: subnets, route tables, firewall rules, Domain Name System (DNS) name resolution, and more

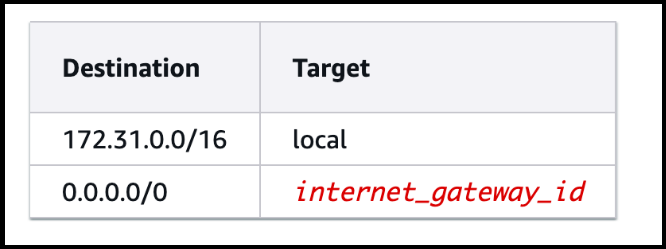
Default VPC



In each Region of your Account a VPC with this configuration is created by default.

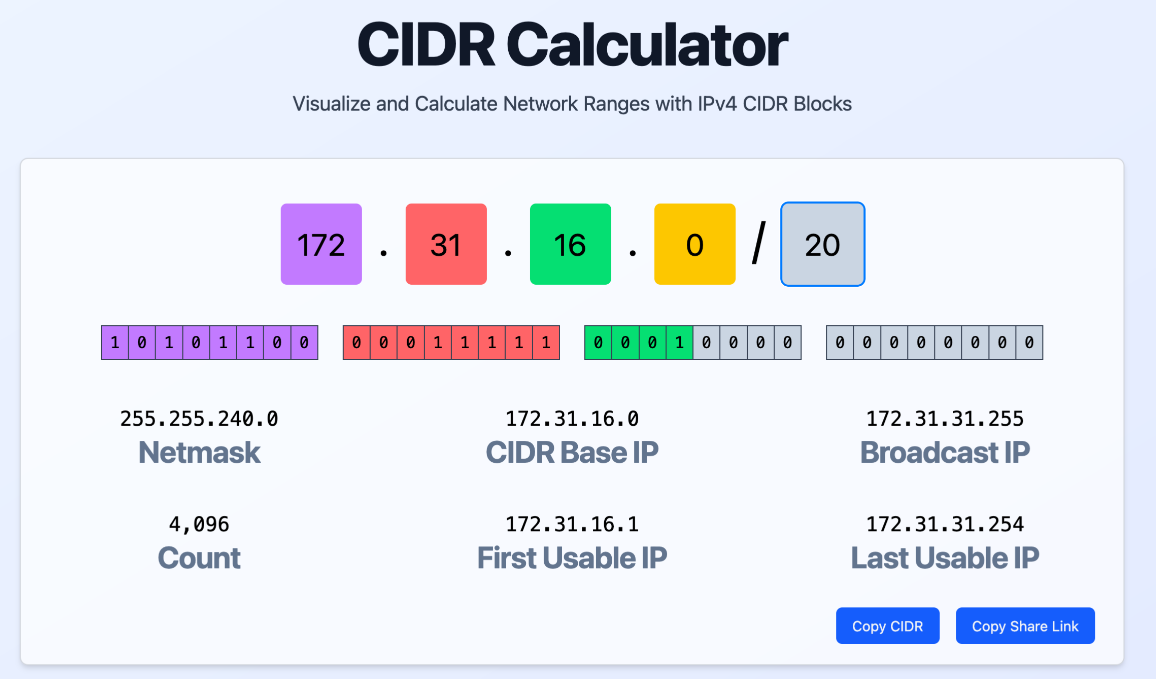
Key points:

- There are three subnets – 1 per AZ. A subnet resides only in a single AZ.
- There is an Internet Gateway (IGW) – access to the Internet is possible.
- There are no components here that cost money!
  - NOTE: That EC2 we created does cost $$$
- The default Route Table entries will allow outbound traffic to the Internet:



Destination	Target
172.31.0.0/16	local
0.0.0.0/0	*internet_gateway_id*

CIDR IP Address Ranges – Classless Inter Domain Routing



CIDR Calculator

Visualize and Calculate Network Ranges with IPv4 CIDR Blocks

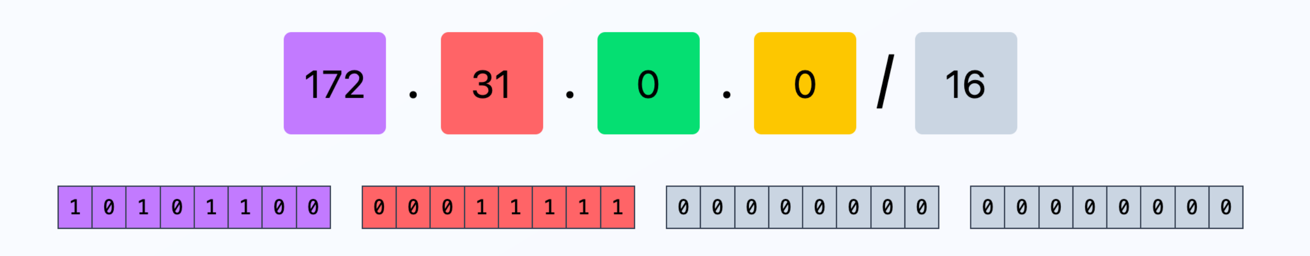
172 . 31 . 16 . 0 / 20

```
1 0 1 0 1 1 0 0   0 0 0 1 1 1 1 1   0 0 0 1 0 0 0 0   0 0 0 0 0 0 0 0
```

255.255.240.0 **Netmask**	172.31.16.0 **CIDR Base IP**	172.31.31.255 **Broadcast IP**
4,096 **Count**	172.31.16.1 **First Usable IP**	172.31.31.254 **Last Usable IP**

Use https://cidr.xyz to get this visual representation of how CIDR addresses are broken down

This /20 Range from a Subnet is "inside" the /16 Range of the VPC



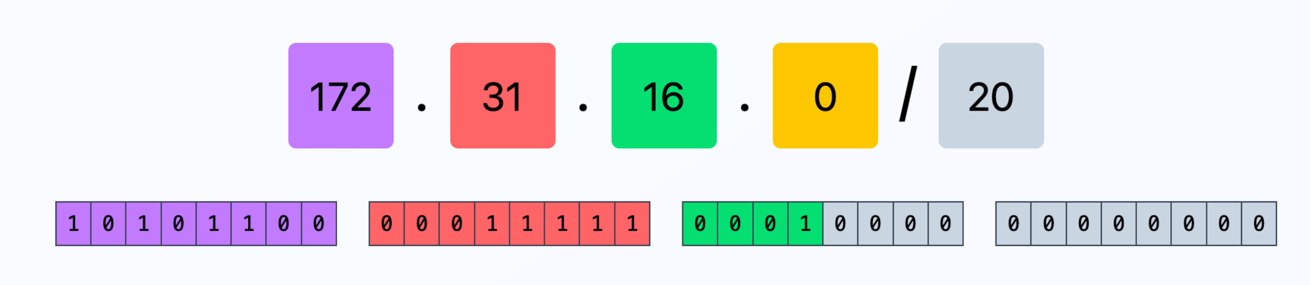
172 . 31 . 0 . 0 / 16

1	0	1	0	1	1	0	0

0	0	0	1	1	1	1	1

0	0	0	0	0	0	0	0

0	0	0	0	0	0	0	0



172 . 31 . 16 . 0 / 20

1	0	1	0	1	1	0	0

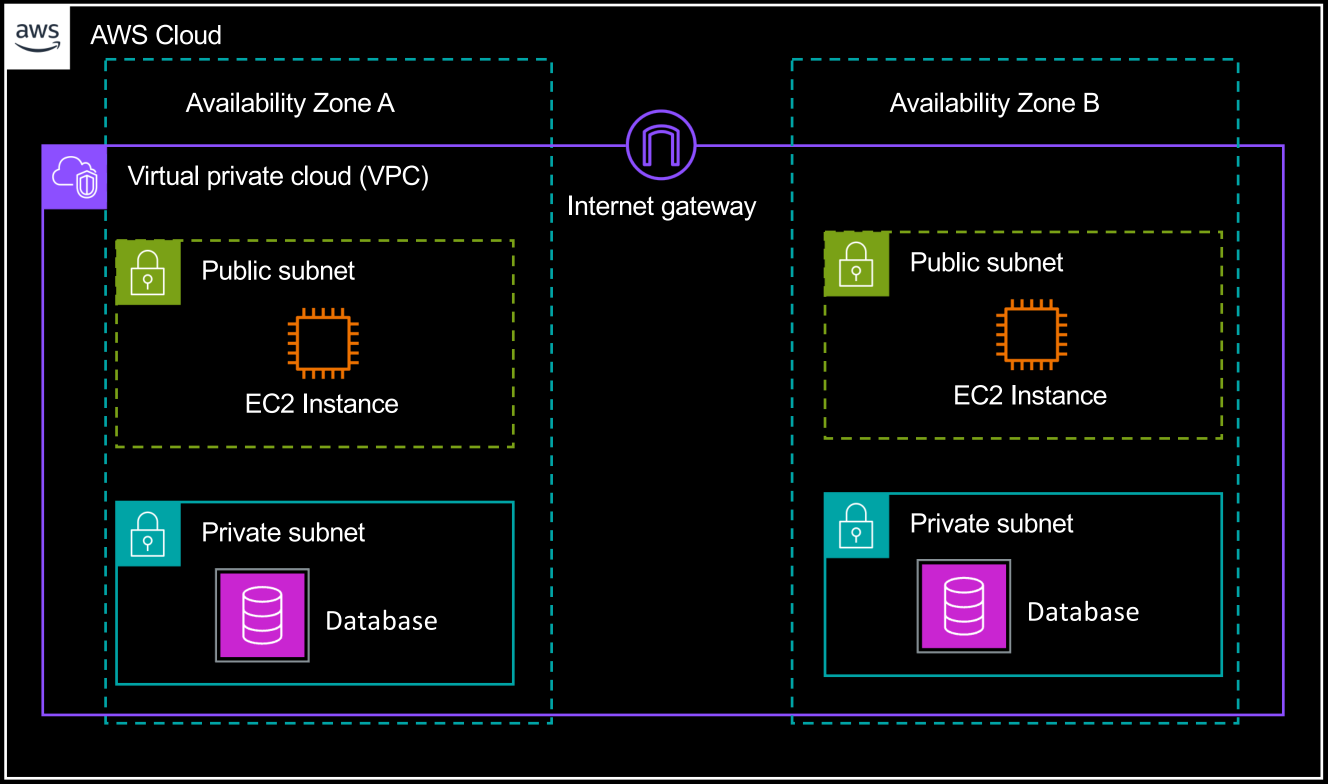
0	0	0	1	1	1	1	1

0	0	0	1	0	0	0	0

0	0	0	0	0	0	0	0

**KEY POINT: A CIDR represents a RANGE of IP addresses –
a /16 is BIGGER (more IPs) than a /20 or /22, etc.**

Don’t use default VPC – this is a better design

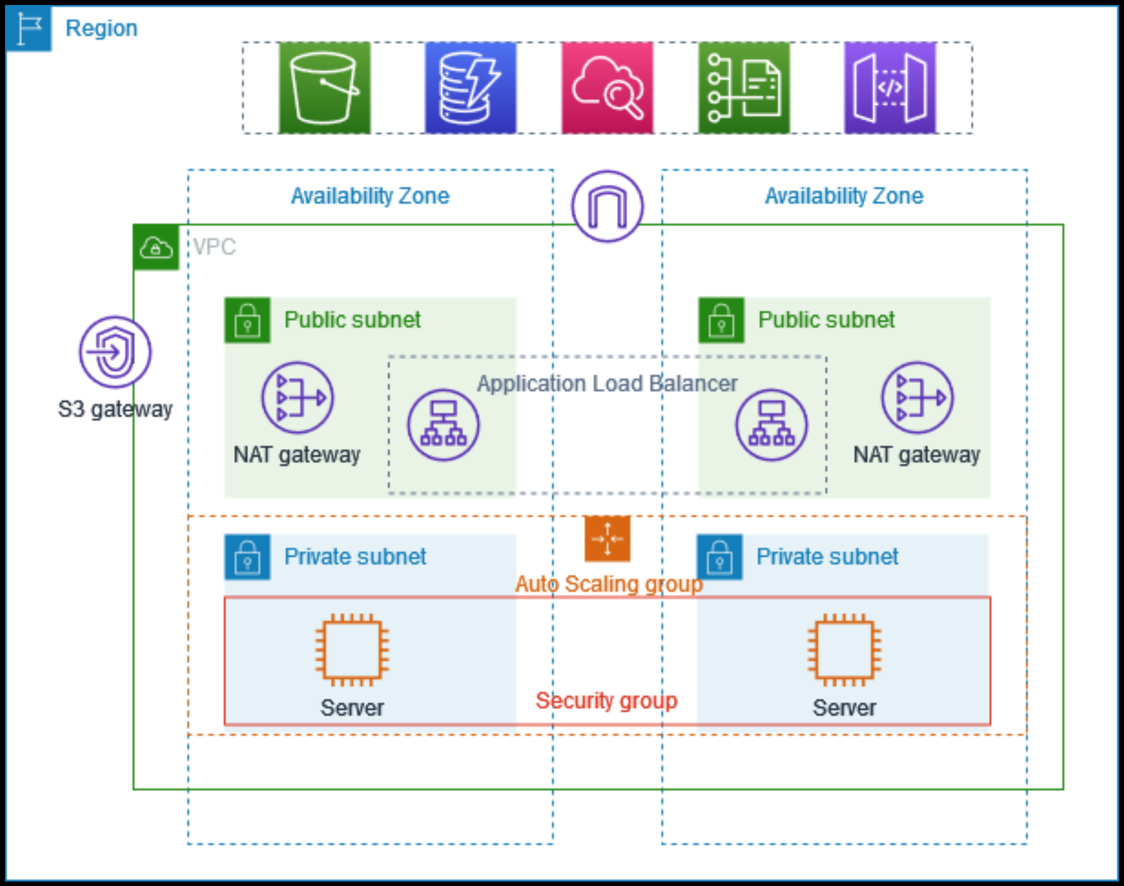


Why?

- Public Subnets for Internet facing resources
- Private Subnets for things that should NEVER be accessible from the Internet
- More than one AZ (Notice the redundancy in the web servers and database nodes.

We are minimizing Single Points of Failure

Another example - with access to AWS services from Private



The servers in Private Subnet can securely access Web Services over the Internet by sending traffic outbound via the **NAT Gateway**

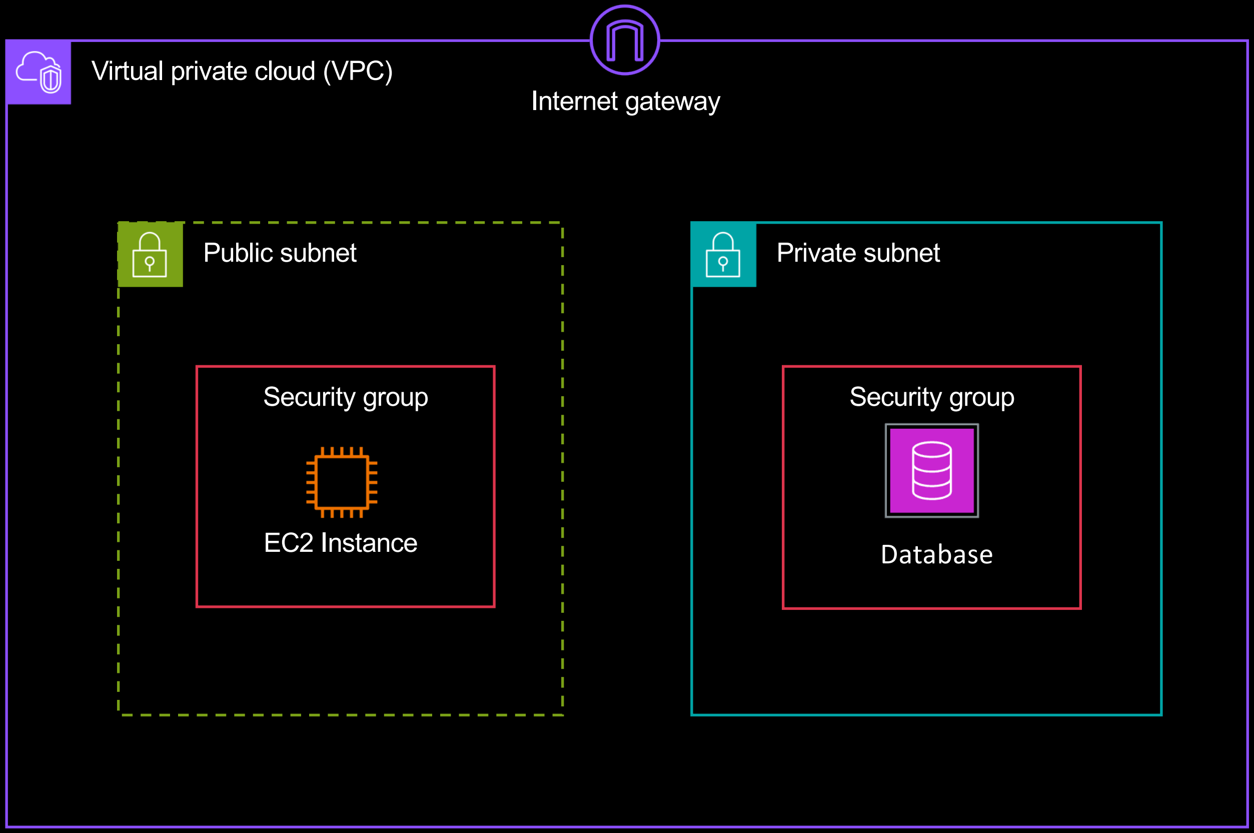
S3, DynamoDB, CloudWatch, etc. are WEB SERVICES.

They are accessed over the INTERNET – that's why they are called WEB Services.

Notice that S3, DynamoDB live in the REGION – NOT in your VPC.

Tutorial to set this up

What about FIREWALL rules?



- Subnets have Network Access Control Lists (ACLs) that protect the entire subnet

- Within the subnet you have Security Groups that let you protect each instance with very specific rules

Why?

- We need to be able to precisely control inbound and outbound traffic
- Not just to the Internet, also within our own VPC
- That's "Defense in Depth"

Links

- CIDR.XYZ: https://cidr.xyz/
- VPC Tutorial (Step by Step): https://docs.aws.amazon.com/vpc/latest/userguide/create-a-vpc-with-private-subnets-and-nat-gateways-using-aws-cli.html
- What is a VPC? https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html
- Security Groups: https://docs.aws.amazon.com/vpc/latest/userguide/vpc-security-groups.html
- Network Access Control Lists: https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html
- Configure Route Tables: https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Route_Tables.html