AWS tual Private Cloud (VPC)

AWS Networking

Table of contents

01 Introduction

02 Key Features

03 Components

04 Subnets

05 IGW

06 Bastion Hosts

07 Nat GW

08 Use Cases

09 Best Practices

01

Introduction

AWS VPC

A VPC is a logically isolated virtual network within the AWS cloud where you can launch AWS resources. You have complete control over your virtual networking environment, including the selection of your IP address range, creation of subnets, and configuration of route tables and network gateways.

02

Key Features

01) Subnetting

1)

Public Subnet

Subnets that are accessible from the internet.

2)

Private Subnet

Subnets that are not directly accessible from the internet.

3)

Isolated

Subnets with no outbound internet access.

02) IP Addresses

- **IPv4 and IPv6 Support:** You can assign both IPv4 and IPv6 addresses to your VPC and its subnets.
- **Customizable CIDR Blocks:** Specify the size and range of your network's IP address space.

03) Routing

1)

Route Tables

Control the traffic between subnets and to the internet.

2)

IGW

Enables communication between your VPC and the internet.

3)

Nat GW

Allow instances in a private subnet to connect to the internet but prevent the internet from connectionlng with those instances.

04) Security

Security Group

Act as a virtual firewall for your instances to control inbound and outbound traffic.

NACLS

Provide an additional layer of security that acts as a firewall for controlling traffic in and out of one or more subnets.

05) Connectivity

- **VPN Connection:** Establish secure connections between your on-premises network and your AWS VPC.

- **Direct Connect:** Provides a dedicated network connection from your premises to AWS.

- **VPC Peering:** Connect VPCs within or across regions to enable communication between them.

06) High Availability & Fault Tolerance

- **Multi-AZ Deployments:** Distribute resources across multiple Availability Zones to achieve high availability and fault tolerance.

- **Elastic IP Addresses:** Static IP addresses designed for dynamic cloud computing.

03

Components

VPC Components

1) VPC

2) Subnets

3) Route Tables

4) IGW

5) Nat GW

6) VPC Peering

7) Elastic IPs

8) Endpoints

04

Subnets

Subnets

Segments of the VPC IP address range where you can place groups of isolated resources. Each subnet must reside entirely within one Availability Zone and cannot span zones.

Subnets

1)

Public Subnet

Subnets with a route to an Internet Gateway.

2)

Private Subnet

Subnets without a direct route to an Internet Gateway. Typically used for backend resources.

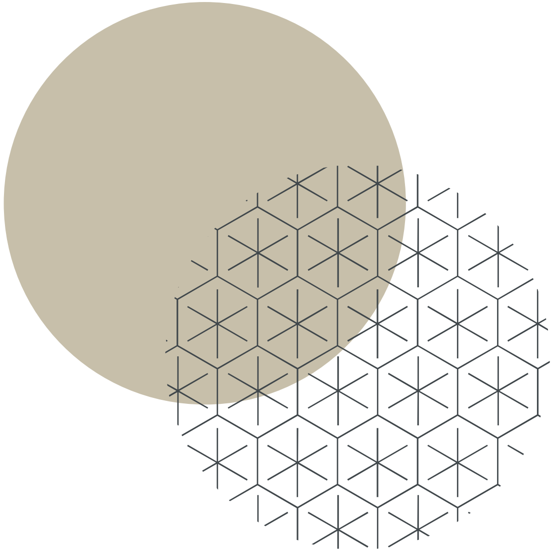
3)

CIDR Blocks

Each subnet has a CIDR block, a subset of the VPC CIDR block.

05

Internet Gateway



IGW

- An IGW allows communication between instances in your VPC and the internet. It horizontally scales, is redundant, and highly available.

IGW

Internet Access

- Required for instances to connect to the internet.

Public IPs

- Instances in public subnets need public IP addresses or Elastic IPs to communicate with the internet.

06

Bastion Host

Bastion Host

A Bastion Host, also known as a Jump Box, is a special-purpose instance that acts as a gateway between a public network and a private network. It provides a secure entry point for administrators to access instances in a private subnet. By using a Bastion Host, you can enhance the security of your network by limiting direct access to your private instances.

07

Nat Gateway

Nat

- These components allow instances in private subnets to connect to the internet or other AWS services, but prevent the internet from initiating connections with those instances.

Nat Instances & Gateways

Nat Instances

- Instances configured to perform NAT functions, requiring manual management.

Nat GW

- Managed service that is more reliable and easier to manage than NAT instances.

08

Use Cases

Use Cases

Hosting Web Applications

Deploy web servers in public subnets, databases in private subnets, and leverage NAT Gateways for secure internet access.

Hybrid Cloud Architectures

Extend your on-premises network to the cloud with secure VPN or Direct Connect connections.

Use Cases

Data Analytics

Use VPC to isolate big data workloads and ensure secure data transfer and processing.

Disaster Recovery

Implement backup and disaster recovery solutions by replicating on-premises data and applications to the VPC.

09

Best Practices

Best Practices

- Design for High Availability:

Use multiple Availability Zones and ensure redundancy for critical components.

- Segment Your Network:

Use public and private subnets to control access to your resources. Isolate critical workloads.

Best Practices

- Security First:

Implement strict security group rules, network ACLs, and regularly audit security configurations.

- Monitor and Log:

Use AWS CloudTrail and VPC Flow Logs to monitor and log network traffic and user activity.

Thanks

Do you have any questions?

mayamnaizel2013@gmail.com
The Tech Stuff

THE TECH STUFF
BY MAYA MNAIZEL

CREDITS: This presentation template was created by **Slidesgo,** including icons by **Flaticon,** infographics & images by **Freepik**