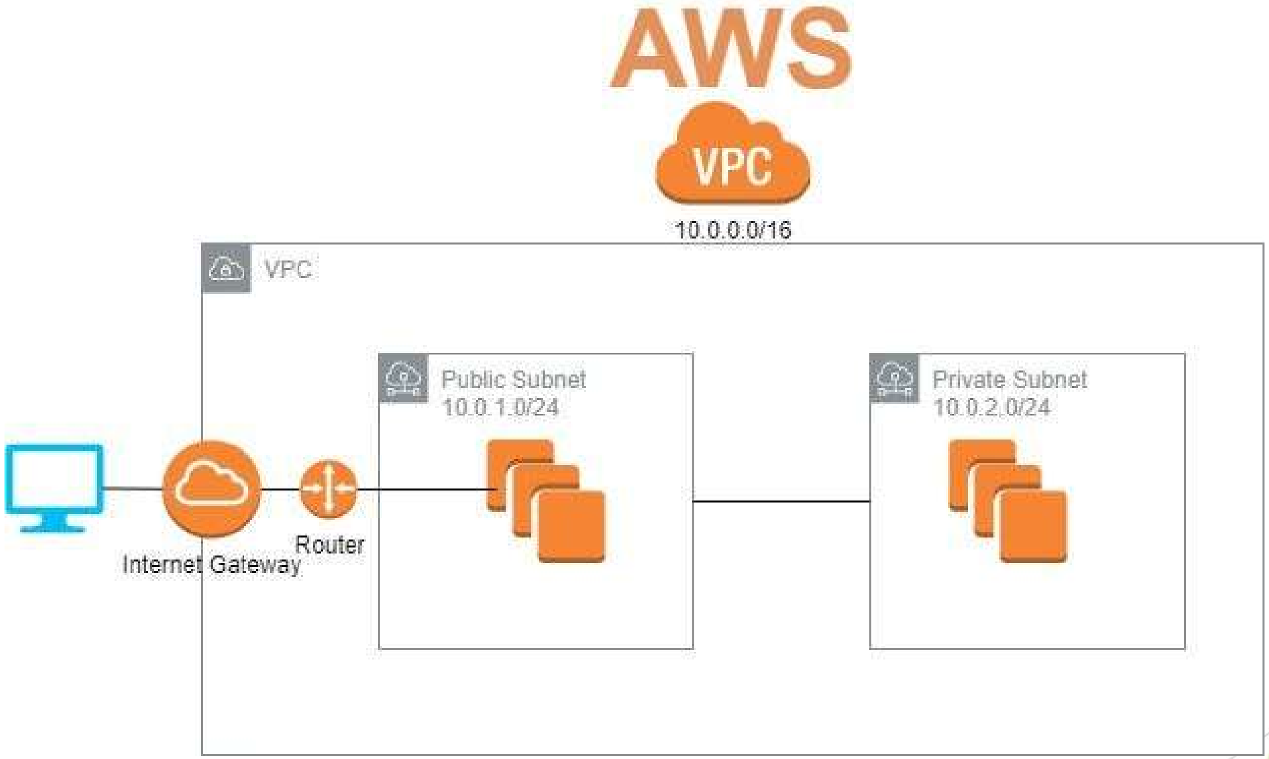
VPC(virtual private cloud)

Presented by Syam_chunduru


AWS
VPC
10.0.0.0/16
VPC
Public Subnet
10.0.1.0/24
Private Subnet
10.0.2.0/24
Internet Gateway
Router

Introduction

- > A VPC is like your own private data center in the cloud, where you can launch and manage AWS resources (like EC2, RDS, etc.) in a secure and customizable network.

Benefits of VPC:

- Security and Isolation
- Customizable Network Configuration
- Scalability and Flexibility
- Control over Network Traffic
- Improved Compliance
- Better Network Management

VPC components

- Subnets: Public and private subnets for resource segregation
- Route Tables: Control traffic routing within the VPC
- Internet Gateway: Enables internet access for public subnets
- NAT Gateway: Allows outbound internet access for private subnets
- Security Groups: Stateful firewall for instance-level traffic control
- Network ACLs: Stateless firewall for subnet-level traffic control

Subnets:

- Public Subnets: - Resources have direct access to the internet - Typically used for resources that need to be accessible from the internet (e.g., web servers)
- Private Subnets: - Resources do not have direct access to the internet - Typically used for resources that should not be accessible from the internet (e.g., databases, backend servers)Key

Route tables:

- A route table determines the routing of traffic within a VPC. It controls the flow of traffic between subnets and out of the VPC.
- Routes: Define the path that traffic takes to reach its destination.
- Targets: Specify the destination of the traffic (e.g., internet gateway, NAT gateway, instance).
- Types:- Main Route Table: Default route table for a VPC.
- - Custom Route Table: User-created route table associated with specific subnets.
- Best Practices:- Control traffic flow and access to resources. Associate route tables with specific subnets.- Regularly review and update route tables.

Security groups:

- Definition: A security group acts as a virtual firewall to control traffic to and from your instances.
- - Key Features:
- Inbound Rules: Control incoming traffic to instances.
- Outbound Rules: Control outgoing traffic from instances.
- Stateful: Security groups track the state of network connections.

Network ACLs in AWS VPC:

- Network Access Control Lists (NACLs) are an important security layer for your Amazon Virtual Private Cloud (VPC) that act as a stateless firewall at the subnet level.
- Key Characteristics of Network ACLs
- 1. *Stateless*: NACLs don't track connection state - you must explicitly allow both inbound and outbound traffic
- 2. *Subnet-level*: Applied at the subnet level (unlike security groups which operate at the instance level)
- 3. *Rule-based*: Process rules in order based on rule numbers
- 4. *Default deny*: Implicit deny for any traffic not explicitly allowed

VPC Best Practices:

- *Design*
- Multi-AZ + non-overlapping CIDR
- Public/Private/Isolated subnets
- *Security*
- SGs (instance) + NACLs (subnet)
- Flow Logs + private DBs
- *Networking*

Peering/PrivateLink > public exposure

NAT per AZ + VPN/DirectConnect + backups

VPC Security:

- Amazon Virtual Private Cloud (VPC) provides the foundation for deploying applications in a secure, isolated, and customizable network environment in the AWS cloud. Security within a VPC is multi-layered, offering several mechanisms to control access to resources and data. This layered approach enables you to implement fine-grained security controls at both the network and instance levels.

Conclusion:

- Amazon VPC serves as the critical networking foundation for your AWS cloud environment, where proper design directly impacts security, performance, and cost efficiency. By implementing strategic subnet segmentation, robust security controls, and multi-AZ redundancy, organizations can build enterprise-grade network architectures that support both current operational needs and future scalability. The most effective VPC implementations follow security-first principles - particularly maintaining strict isolation for sensitive workloads - while leveraging AWS's native networking services for optimal connectivity. Remember that VPC management is an ongoing process requiring continuous monitoring, periodic reviews of access controls, and optimization to eliminate unnecessary costs. When executed well, a properly configured VPC provides the secure, high-performance network backbone that enables all other AWS services to function at their best while maintaining compliance with organizational and regulatory requirements.