AWS Cloud Subnet and Access

Topics : AWS
Written on December 08, 2023

In Amazon Web Services (AWS), subnets are subdivisions of a Virtual Private Cloud (VPC) IP address range where you can place groups of resources. Subnets allow you to segment and organize your network resources within a VPC. Additionally, controlling access to resources within subnets is crucial for network security. Let's explore subnets and access control in AWS:

Subnets in AWS:

1. **Definition:**
   - A subnet is a range of IP addresses in your VPC.
   - Subnets are created within a VPC and are associated with a specific availability zone.
2. **IP Addressing:**
   - Subnets have their own IP address range, a subset of the overall VPC CIDR block.
3. **Public and Private Subnets:**
   - **Public Subnet:** Typically associated with resources that need direct access to the internet. Instances in a public subnet might have Elastic IP addresses or public IP addresses.
   - **Private Subnet:** Reserved for resources that do not require direct internet access. Instances in a private subnet can access the internet through a Network Address Translation (NAT) gateway or NAT instance.
4. **Route Tables:**
   - Each subnet is associated with a route table, which controls the traffic leaving the subnet.
   - Public subnets typically have a route to an Internet Gateway (IGW) for direct internet access.
5. **Network ACLs and Security Groups:**
   - **Network ACLs (NACLs):** These act as a firewall for controlling traffic in and out of a subnet.
   - **Security Groups:** These are stateful firewalls associated with instances. They control inbound and outbound traffic at the instance level.

ARYATECHNO

Access Control in AWS:

1. **Security Groups:**
    - **Definition:** Security Groups act as virtual firewalls for your instances.
    - **Inbound Rules:** Define what traffic is allowed to reach your instances.
    - **Outbound Rules:** Define what traffic is allowed to leave your instances.
2. **Network ACLs (NACLs):**
    - **Definition:** NACLs are stateless and control traffic at the subnet level.
    - **Inbound and Outbound Rules:** Specify rules for allowing or denying traffic based on IP addresses, protocols, and ports.
3. **Route Tables:**
    - **Definition:** Route tables determine where network traffic is directed.
    - **Public and Private Routes:** Define routes to IGW for public subnets and NAT gateways or instances for private subnets.
4. **Internet Gateway (IGW):**
    - **Definition:** An IGW allows communication between instances in your VPC and the internet.
    - **Associated with Public Subnets:** Typically associated with public subnets to enable direct internet access.
5. **NAT Gateway or NAT Instance:**
    - **Definition:** NAT gateways or instances enable instances in private subnets to initiate outbound traffic to the internet while preventing inbound traffic.
    - **Private Subnet Access:** Used for instances in private subnets that need internet access (e.g., for software updates).
6. **Elastic IP Addresses (EIPs):**
    - **Definition:** EIPs are static IP addresses that can be associated with instances in a VPC.
    - **Public IP Addresses:** Instances in a public subnet can have public EIPs or public IPs.
7. **VPN and Direct Connect:**
    - **VPN (Virtual Private Network):** Provides secure communication between your on-premises data center and your VPC.
    - **Direct Connect:** Offers dedicated network connections between your on-premises environment and AWS.
8. **Amazon VPC Peering:**
    - **Definition:** VPC peering allows communication between instances in different VPCs.
    - **Inter-VPC Connectivity:** Enables resource sharing and communication between different VPCs.

ARYATECHNO

9. **AWS PrivateLink:**
    - **Definition:** AWS PrivateLink allows access to services over the AWS backbone network rather than the public internet.
    - **Secure Access:** Enhances security by avoiding exposure to the public internet.

© Copyright **Aryatechno**. All Rights Reserved. Written tutorials and materials by Aryatechno

ARYATECHNO