Building and Securing AWS Networks

Cloud Practitioner Essentials

JUNE 2024

ISSUED BY
Medha Prodduturi

What is AWS Cloud Networking?

AWS offers various cloud services and AWS Networking Services act as the building blocks that connect these services together. These networking services work together to provide a secure, scalable, and highly available network infrastructure. Thus, in order to design an efficient network architecture for your cloud applications, it is important to understand how these networking services work.

In this article:

Core Concepts of AWS Networking

Amazon VPC

Amazon Virtual Cloud Service (VPC) is a foundational concept for secure cloud networking. It is a service that allows you to launch AWS resources in an isolated virtual network. This virtual network is hidden from the outside world, allowing you to perform operations that you don't want to make public. It provides you with a private address space and a configurable firewall to control traffic flow. After you create a VPC, you can add subnets.

Subnet

A subnet is a range of IP addresses within a VPC and acts like a subsection of your virtual network. In each subnet, you can create AWS resources such as EC2 instances and can identify every subnet through a unique id provided by AWS. While VPC spans across the entire Region, every subnet can only be associated with one Availability Zone.

The type of subnet is determined by how you configure their routing. There are different types of subnets:

1. **Private Subnet** - The subnet does not have a direct route to an internet gateway. To access the resources, they require a NAT device to access the public internet.
2. **Public Subnet** - The subnet has a direct route to an internet gateway (IGW). Resources in a public subnet can directly access and be accessed from the internet (if security groups allow).
3. **VPN-only Subnet** - This subnet does not have a direct route to the internet gateway but has a route to a virtual private gateway (VGW) in your VPC. THE VGW can connect to a VPN connection, allowing resources in the subnet to securely communicate with your on-premises network over the internet.
4. **Isolated Subnet** - The subnet has no routes to outside its VPC. Resources in an isolated subnet can only communicate with other resources within the same VPC and subnet. This is the most secure option, but it also restricts communication options.

Routing and Internet Gateways

Route Tables

A route table is a central traffic management system within the VPC; it contains a set of rules called routes that determine where the network traffic from your subnet or gateway is directed. It then directs those resources to the right destinations based on predefined values. Using route tables, you can ensure that resources are efficiently reaching their destinations through the most optimal path.

Internet Gateway (IGW)

The resources in your public subnets can connect to the internet if the resources have a public IPv4 or an IPv6 address with the help of an internet gateway. Internet resources can also initiate connection to subnet resources using the public IPv4 or IPv6 address.

Virtual Private Gateway (VGW)

For a VPC that only consists of private resources, we use a Virtual Private Gateway (VGW). VGW allows you to establish a Virtual Private Network (VPN) connection between your network and the VPC so that you can extend your on-premises network into the cloud seamlessly and with increased security.

AWS Direct Connect

Although the VPN connections of VGW are private and encrypted, they still use regular internet connections whose bandwidth is shared by many users of the internet. This process is susceptible to slowdowns; thus, to make it even more reliable and faster, we use AWS Direct Connect.

This cloud service is the shortest path to your AWS resources and remains on the AWS global network while in transit, never touching the public network. It lets you establish a completely private and dedicated connection from your data center to AWS, combatting any bandwidth, compliance, and latency issues altogether.

Security Groups and Network ACLs

Security Groups

You know that a subnet can contain resources like EC2 Instances. A security group is assigned to each instance and acts as a firewall which controls the inbound and outbound traffic for the instance. The rules of a security group control the inbound traffic, but by default, the security groups contain outbound rules that allow all

outbound traffic. However, these rules can be deleted or created separately. Multiple resources within the same VPC can be associated with the same security group or can have different security groups for each of them.

Security Groups are stateful. This means that they keep track of existing connections and automatically allow the corresponding return traffic without needing an explicit rule for it.

Network ACLs

Network Access Control Lists (ACLs) act as an additional layer of security that governs the traffic flow at the subnet level within your VPC; they are associated with subnets, not individual resources like security groups. All traffic that enters or leaves a subnet is subject to the rules defined in its associated network ACL.

Network ACLs are stateless. They evaluate each packet of data independently without considering existing connections. Meaning, each time a packet enters or leaves, ACL will check for permissions regardless of whether the packet has entered previously.

Summary

Imagine your company is building a new office building within the entire office complex (in our case, this is the AWS Cloud). Below is how different features we discussed so far fit into this analogy.

Feature	Analogy
Virtual Private Cloud (VPC)	Isolating your resources from others by creating separate walls within your office space.
Subnet	Departments within your office that have their own set of desks (IP addresses) for employees (resources) to work at.

Route Tables	A receptionist that directs visitors (data packets) to the correct department (subnet) within the building.
Internet Gateway (IGW)	The main gate of the building complex which allows people (data) to enter and exit.
Virtual Private Gateway (VGW)	A secure gateway within your office building that allows only authorised entrances to departments.
AWS Direct Connect	A dedicated optic line installed from your company's headquarters to your office building.
Security Groups	Security guards stationed at each department entrance (subnet) that control who can access individual offices (resources) within a department.
Network Access Control List (ACL)	Security checkpoints at the building's main entrance that control who can enter specific departments (subnets) within the building.

Next Step

To dive deeper into specific services, explore the AWS documentation for more granular details and best practices. Take advantage of AWS hand-on tutorials to experiment and gain practical experience in setting up your own VPC environment.