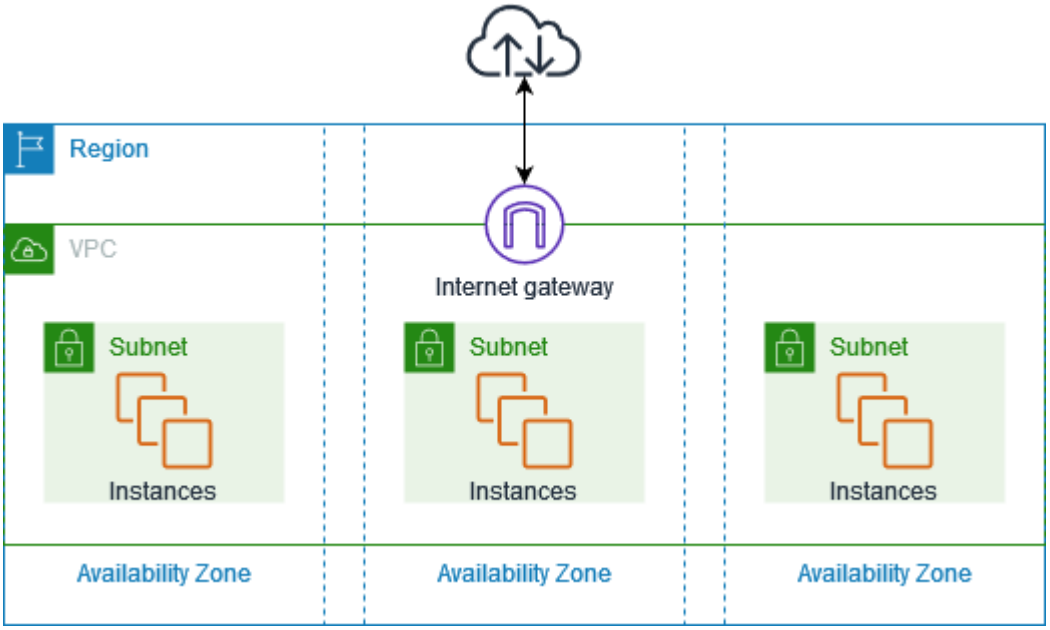
What is Amazon VPC?

https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html

VPC(Virtual Private Cloud) provides you isolated network to host your own resources according to your use case on the AWS cloud. It empowers you to create a virtual cloud that is fully configured, either private or public, as per your needs.

However, AWS lets you configure the networking of VPC and its resources, but there is a recommended framework, AWS Well-Architected Framework, which enables you to configure a secure, resilient, and Highly Available virtual Data Center.



Features

Subnets

A subnet is a range of IP addresses in your VPC. A subnet must reside in a single Availability Zone. After you add subnets, you can deploy AWS resources in your VPC.

IP Addressing

You can assign IP addresses, both IPv4 and IPv6, to your VPCs and subnets. You can also bring your public IPv4 addresses and IPv6 GUA addresses to AWS and allocate

them to resources in your VPC, such as EC2 instances, NAT gateways, and Network Load Balancers.

Routing

Use route tables to determine where network traffic from your subnet or gateway is directed.

Gateways and endpoints

A gateway connects your VPC to another network. For example, you can use an internet gateway to connect your VPC to the Internet. Alternatively, you can use a VPC endpoint to connect to AWS services privately without the use of an internet gateway or NAT device.

Peering connections

Use a VPC peering connection to route traffic between the resources in two VPCs.

Traffic Mirroring

Copy network traffic from network interfaces and send it to security and monitoring appliances for deep packet inspection.

Transit gateways

Use a transit gateway, which acts as a central hub, to route traffic between your VPCs, VPN connections, and AWS Direct Connect connections.

VPC Flow Logs

A flow log captures information about the IP traffic going to and from network interfaces in your VPC.

VPN connections

Connect your VPCs to your on-premises networks using AWS Virtual Private Network (AWS VPN).

Pricing for Amazon VPC

There's no additional charge for using a VPC. There are, however, charges for some VPC components, such as NAT gateways, IP Address Manager, traffic mirroring, Reachability Analyzer, and Network Access Analyzer.

Public IPv4 addresses

Public IPV4 addresses are routable on the internet; any resources that need to be connected to the internet must have Public IPv4 addresses.

Any public IPv4 addresses provisioned to your account by the managed service will be charged. These charges will be associated with the Amazon VPC service in your AWS Cost and Usage Report.

Private IPv4 addresses (RFC 1918) are not charged.

Types of Public IPV4 Addresses

Elastic IP Addresses: Elastic IP addresses are persistent public IP addresses assigned to resources to connect to the Internet; they don't change until they are removed from the AWS account.

EC2 Public IPv4 addresses: It is assigned to EC2 instances if an EC2 instance is launched in a default subnet or an automatically assigned public IP is configured to the subnet. Once EC2 is rebooted, these IP addresses can be changed.

BYOIPv4 Address: You can use your own public IPv4 addresses into AWS resources. https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-byoip.html

Service Managed IP addresses: AWS services create a public IPv4 address to connect with the internet, and it is managed by AWS.

By default, one route table will be created with the VPC, and it is associated with the subnet level.

How Amazon VPC works

Default VPC and nondefault VPCs

In your AWS account, there is one default VPC created in each region, in which one default subnet is created in each Availability zone in the region.

- A route in the main route table that sends all traffic to the internet gateway.
- DNS settings that automatically assign public DNS hostnames to instances with public IP addresses and enable DNS resolution through the Amazon-provided DNS server (see DNS attributes for your VPC)

Route Tables

A set of route rules is called a route table. To manage the outbound traffic from a subnet, one route table should be associated with the subnet; otherwise main route table will be implicitly associated with the subnet.

Access the Internet

If your resources are created in the default subnet, then it is connected to the internet by default. If you create ec2 instance in a non-default subnet VPC, then you can use below ways to allow ec2 instance to access the internet.

Use the Internet gateway if your resource is created in a nondefault VPC.
Use NAT Gateway to allow only outbound traffic but prevent inbound traffic.

If you associate an IPv6 CIDR block with your VPC and assign IPv6 addresses to your instances, instances can connect to the internet over IPv6 through an internet gateway.

Alternatively, instances can initiate outbound connections to the internet over IPv6 using an egress-only internet gateway. IPv6 traffic is separate from IPv4 traffic; your route tables must include separate routes for IPv6 traffic.

An internet gateway enables your instances to connect to the internet through the Amazon EC2 network edge

Access a corporate or home network

You can optionally connect your VPC to your own corporate data center using an IPsec AWS Site-to-Site VPN connection, making the AWS Cloud an extension of your data center.

A Site-to-Site VPN connection consists of two VPN tunnels between a virtual private gateway or transit gateway on the AWS side and a customer gateway device located in your data center. A customer gateway device is a physical device or software appliance that you configure on your side of the Site-to-Site VPN connection.

- AWS Site-to-Site VPN User Guide
- Amazon VPC Transit Gateways

Connect VPCs and networks

You can create a *VPC peering connection* between two VPCs that enables you to route traffic between them privately.

You can also create a *transit gateway* and use it to interconnect your VPCs and on-premises networks. The transit gateway acts as a Regional virtual router for traffic flowing between its attachments, which can include VPCs, VPN connections, AWS Direct Connect gateways, and transit gateway peering connections.

- Amazon VPC Peering Guide
- Amazon VPC Transit Gateways

AWS operates our backbone network to target a p99 of the hourly PLR of less than 0.0001%.