Amazon Virtual Private Cloud (AWS VPC)

AWS VPC is one of the most popular and widely used services of Amazon Web Services. This is generally because Amazon VPC is mostly related to the security concepts in the cloud and access to the data inside a third-party data center. AWS VPC is a private subsection of AWS in which you can place AWS resources such as EC2 instances and databases. You have full control over who has access to the resources that you place inside the AWS Virtual Private Cloud.

Overview

- Virtual Private Cloud (VPC) is a logically isolated network from another virtual network in the AWS cloud where you can launch the AWS resources.
- It gives all the benefits of the traditional network that you have for your own data center.
- Resources and applications are accessed through IPv4 or IPv6 in your AWS VPC.
- It gives the benefit of scalable infrastructure in the AWS environment.
- It gives you complete control over your virtual network.

VPC vs Private Cloud

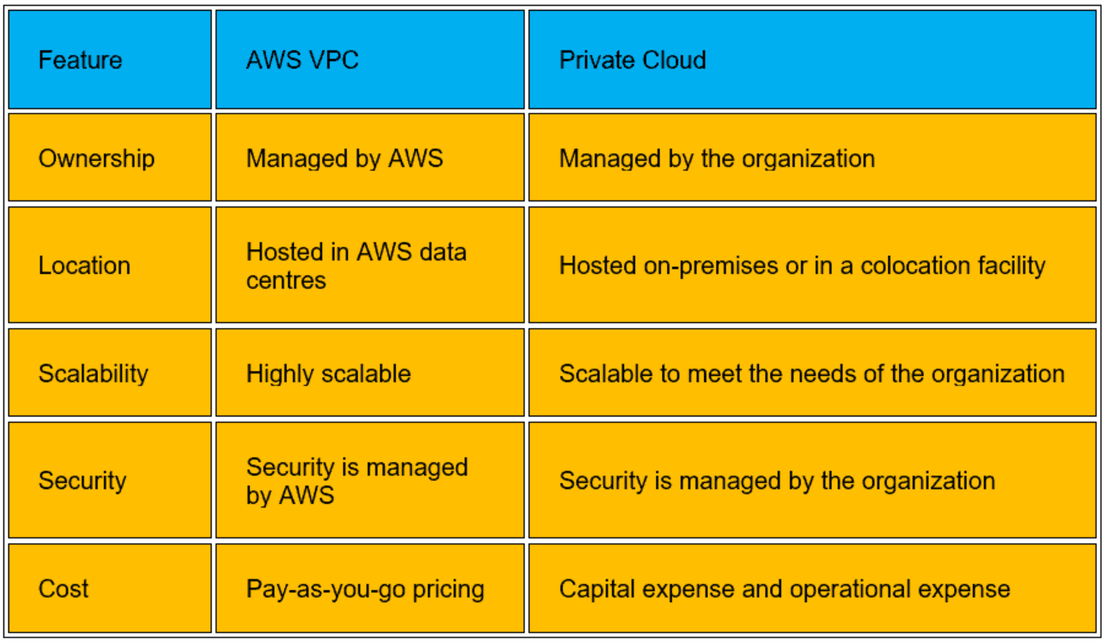
AWS VPC is a public cloud service that provides a private cloud-like experience, whereas a private cloud is a dedicated cloud environment hosted on-premises or in a colocation facility.

The following table summarises the main differences between AWS VPC and private cloud:

VPC vs Private Cloud

AWS VPC is a public cloud service that provides a private cloud-like experience, whereas a private cloud is a dedicated cloud environment hosted on-premises or in a colocation facility.

The following table summarises the main differences between AWS VPC and private cloud:



Feature	AWS VPC	Private Cloud
Ownership	Managed by AWS	Managed by the organization
Location	Hosted in AWS data centres	Hosted on-premises or in a colocation facility
Scalability	Highly scalable	Scalable to meet the needs of the organization
Security	Security is managed by AWS	Security is managed by the organization
Cost	Pay-as-you-go pricing	Capital expense and operational expense

Types of AWS VPCs in AWS Cloud

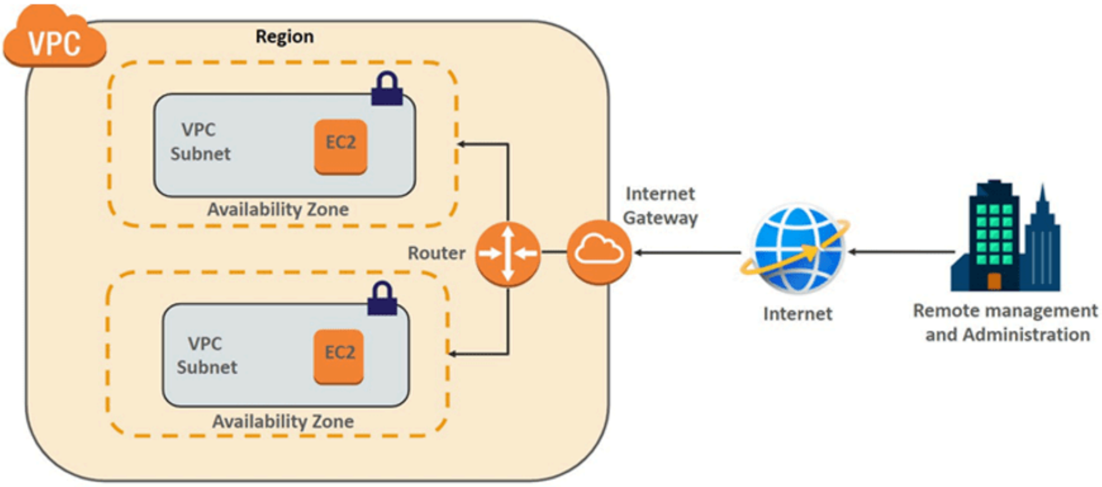
1. Default VPC
2. Non-default VPC

The **default VPC** is a virtual network that is automatically created for the customer's AWS account when EC2 resources are provisioned for the first time. A **non-default** (also known as Customer VPC) is not created automatically when EC2 resources are provisioned, and the customer must create their own VPC. The AWS system automatically creates the default VPC, whereas the customer/nondefault VPC must be manually configured by each customer and resources must be provisioned. When a new instance is launched without first allocating a subnet, the Default VPC is assigned.

Another significant advantage of **Default VPC** is that it includes Internet access by default, as well as an internet gateway and public subnets with corresponding route tables. This feature is not enabled by default in non-default VPC. In fact, in **non-default VPCs**, public IPv4 addresses are not assigned. In terms of numbers, only VPC is available per region, whereas customer VPC is limited to 5 by default for each region.

Benefits Of Using AWS Virtual Private Cloud

- EC2 Instance security group membership can be changed while it is running.
- Static IPv4 is assigned to Instances that persist across the start and stop.
- Create a layered network of resources.
- A single-tenant hardware option is available to run EC2 Instances.
- Access Control List (ACL) is an additional security layer to protect Instances.
- Multiple IPv4 can be assigned to your Instances.
- Control both inbound and outbound traffic of Instances.
- Multiple network interfaces can be attached to EC2 Instances.



Components of AWS VPC

- **Route Table:** In AWS Virtual Private Cloud, route Tables are the set of rules, that are used to determine where the network traffic has to be directed. The route table specifies the destination (IP address) and target (where do want to send the traffic to that destination). The target can be an Internet gateway, NAT gateway, Virtual private gateway, VPC peering connection, etc
- **Subnet:** It is a portion of the network that shares a common address component. All devices whose addresses have the same prefix are in the same subnet. For example, all those devices whose IP address would start with 172.31.1 would be part of the same subnet. There are two

types of subnets. **Private Subnet** where resources are not exposed to the outside world and **Public Subnet** where resources are exposed to the internet through Internet Gateway.

- **Security Groups:** Security groups are a set of firewall rules that controls the traffic for your instance. In Amazon Firewall the only action that can be carried out is allowed. You cannot create a rule to deny. The destination is always the instance on which the service security group is running. You can have a single security group associated with multiple instances.
- **NAT Gateway:** Network Address Translation (NAT) Gateway is used when higher bandwidth and availability with lesser administrative effort is required. NAT gateway always resides inside the public subnet of an Availability Zone. It updates the routing table of the private subnet such that it sends the traffic to the NAT gateway. Elastic IP must be attached to the NAT gateway while creating. It supports only TCP, UDP, and ICMP protocols.
- **VPC Peering:** A VPC peering connection allows you to route traffic between two Virtual Private Cloud's using IPv4 or IPv6 private addresses. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account. A VPC peering connection helps you to facilitate the transfer of data
- **Network Access Control Lists (NACL):** an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. You might set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC. The default network ACL is configured to allow all traffic to flow in and out of the subnets to which it is associated.
- **Virtual Private Gateway:** A virtual private gateway is the VPN concentrator on the Amazon side of the VPN connection. You create a virtual private gateway and attach it to the VPC from which you want to create the VPN connection.
- **Customer Gateway:** An Amazon VPC VPN connection links your data center (or network) to your Amazon VPC (virtual private cloud). A customer gateway is an anchor on your side of that connection. It can be a physical or software appliance.
- **Elastic IP:** It is a static IP address that never changes and is a reserved public IP address that can be assigned to any Instance in a particular region. An elastic IP is reserved for your AWS account and is yours until you release it.
- **Network Interface:** Network Interface is a point of connection between a public and a private network. Every instance has a default network interface, called the primary network interface. Network traffic is automatically shifted to the new instance if you move it from one instance to the other.
- **VPC Endpoints:** VPC endpoints allow private connection between your AWS VPC and other AWS services without using the internet. VPC endpoint devices are scaled, redundant, and highly available VPC components. There are two types of AWS Virtual Private Cloud endpoints **Interface endpoints** and **Gateway Endpoints.**

Best Practices For Securing Your AWS VPC Implementation

Running a machine with mission-critical workloads requires multiple layers of security. Amazon Virtual Private Cloud can be secured like your on-premises data center by following some of these useful tips:

- Amazon Web Services marketplace offers you a web application firewall, a firewall virtual appliance, and a few other tools which you can use to secure your Amazon VPC.
- To secure your protocols from unauthorized access you can configure intrusion detection systems and intrusion prevention virtual appliances.
- With the help of Configure Privileged Identity access management, you can audit and monitor Administrator access to your VPC.
- For transferring information securely between Amazon VPC among diverse regions or Amazon VPC to an on-premises data center, you can easily configure a Site-to-Site VPN.

- Another option to transfer information securely is to use AWS Transfer for Secure File Transfer Protocol (AWS SFTP). With AWS SFTP, you use VPC endpoints and avoid using public IP addresses or going through the internet. In addition, VPC endpoints for AWS SFTP leverage security functionality via AWS private link, which provides private connections between your VPCs and AWS services.

AWS VPC Pricing

Amazon VPC Traffic Mirroring Pricing

If you choose to enable traffic mirroring on the Elastic Network Interface (ENI) of Amazon EC2 instances, you will be charged hourly for each ENI that is enabled with traffic mirroring. If you no longer wish to be charged for traffic mirroring, simply disable traffic mirroring on EC2 instance ENIs using the AWS Management Console, command-line interface, or API. The hourly price per ENI is: $0.015

NAT Gateway Pricing

- **NAT Gateway Hourly Charge:** NAT Gateway is charged on an hourly basis. For this region, the rate is $0.045 per hour.
- **NAT Gateway Data Processing Charge:** 1 GB of data went through the NAT gateway. The NAT Gateway Data Processing charge is applied and will result in a charge of $0.045.
- **Data Transfer Charge:** This is the standard EC2 Data Transfer charge. 1 GB of data was transferred from the EC2 instance to S3 via the NAT gateway. There was no charge for the data transfer from the EC2 instance to S3 as it is Data Transfer Out to Amazon EC2 to S3 in the same region.

AWS VPN pricing

If you create an AWS Site-to-Site VPN connection to your Amazon VPC, you are charged for each VPN connection hour i.e. $0.05 per Site-to-Site VPN connection per hour

AWS provides a number of efficient, secure connectivity options to help you get the most out of AWS when integrating your remote networks with Amazon VPC. AWS Virtual Private Cloud enables you to launch AWS resources into a virtual network that you've defined. This virtual network closely resembles a traditional network that you would operate in your own data center, with the benefits of using the scalable infrastructure of AWS.

VPC Creation Steps:

Step 1 - Create a VPC with CIDR Range 10.0.0.0/16
Step 2 - Create one Public Subnet and one Private Subnet
Step 3 - Create two Route Tables. One for Public Subnet and another for Private Subnet
Step 4 - Associate the Public RT with Public Subnet and associate the Private RT with Private Subnet
Step 5 - Create a Internet Gateway and attach it to VPC
Step 6 - Specify the IGW in the Public RT (0.0.0.0/0 to IGW)
Step 7 - For internet to Private Subnet, Create a NAT Gateway in Public Subnet and route the 0.0.0.0/0 of private Subnet to NAT GAW in Private RT