Amazon Virtual Private Cloud (AWS VPC) – Overview, Benefits & Components

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.

Types of AWS VPCs in AWS Cloud

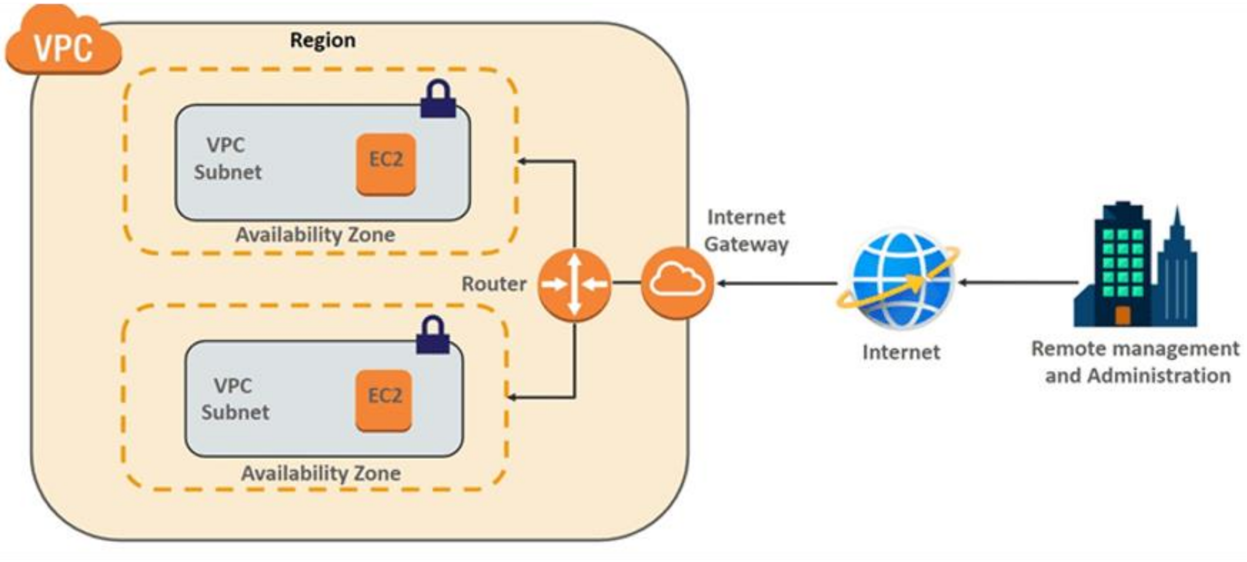
1. Default VPC
2. Non-default VPC

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.

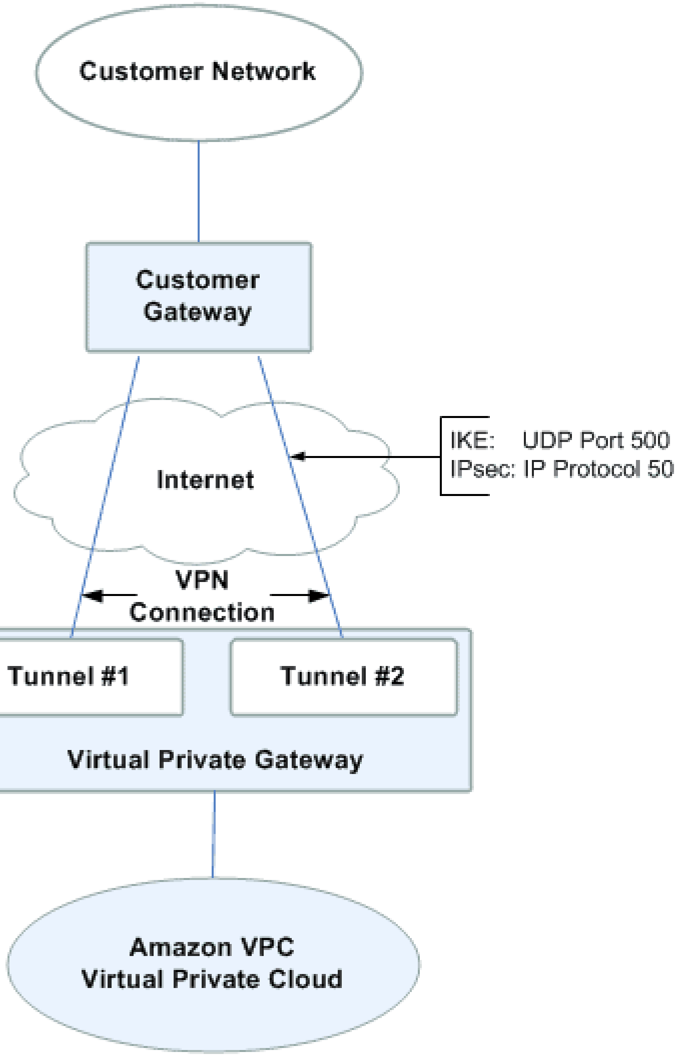


Components of AWS VPC

- **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.**

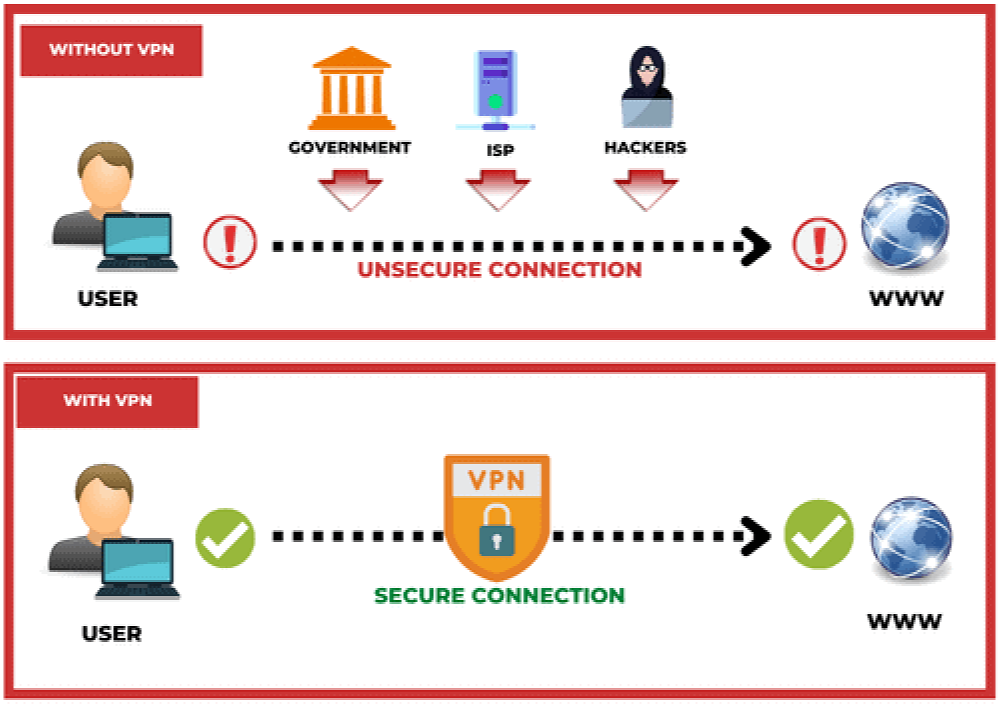


AWS Virtual Private Network (AWS VPN

AWS Virtual Private Network (AWS VPN) creates a secure and private tunnel between your network or
device and the AWS Cloud. You can connect to additional AWS resources from a client or expand your current on-premises network into a VPC.

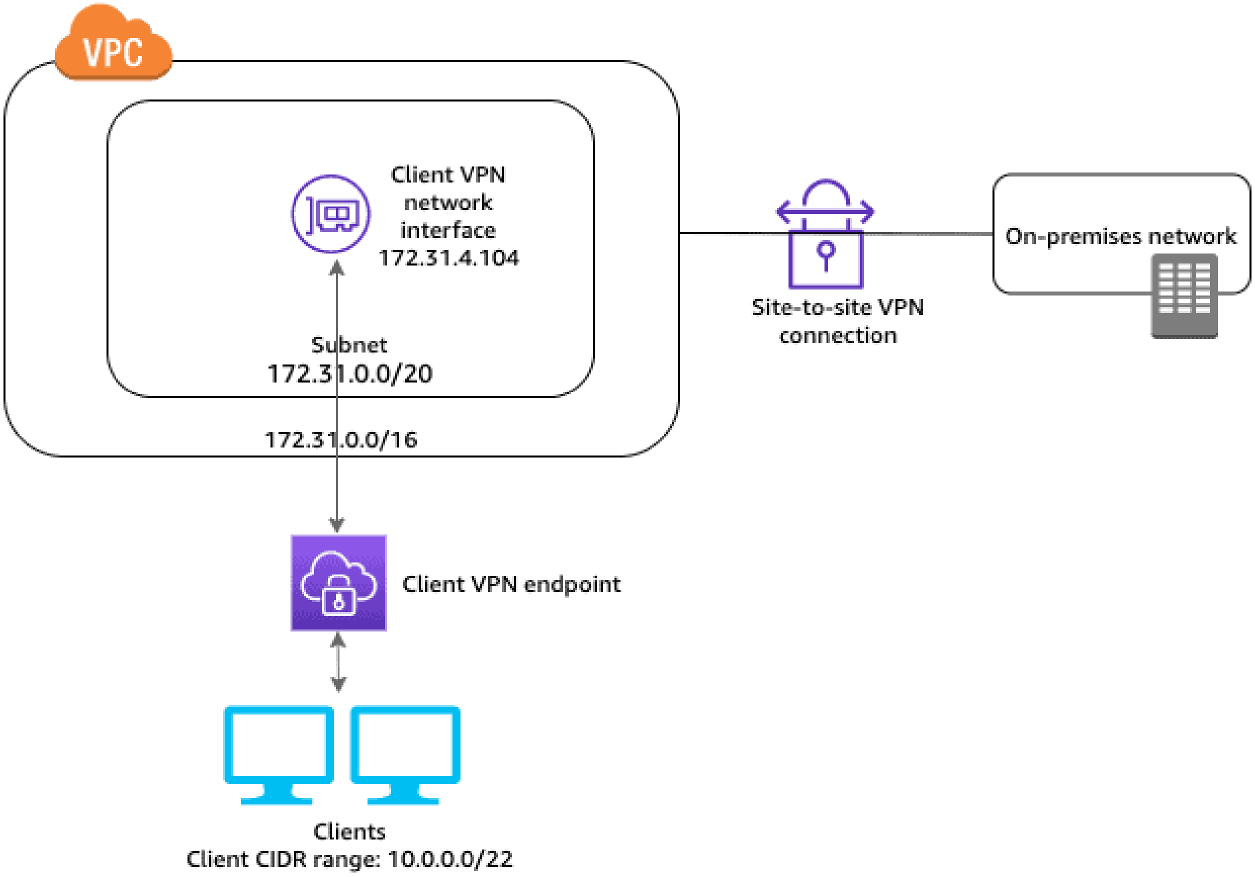
What is Virtual Private Network?

VPN **(Virtual Private Network)** refers to the ability to establish a secure network connection when using public networks. VPNs mask your online identity and encrypt your internet activity. This makes it more challenging for outside parties to monitor your internet activities and steal data. **Real-time** encryption is employed.

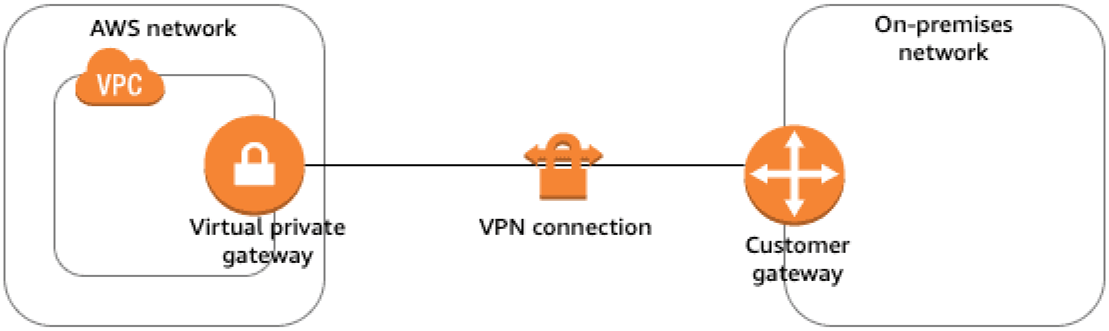


What is AWS VPN?

AWS Virtual Private Network (VPN) solutions connect your on-premises networks, distant offices, client devices, and the AWS global network in a secure manner. AWS Client VPN and AWS Site-to-Site VPN are the two services that make up this system. Each service offers a managed, scalable, and highly available cloud VPN solution to secure your network traffic.


VPC
Client VPN network interface 172.31.4.104
Subnet 172.31.0.0/20
172.31.0.0/16
Site-to-site VPN connection
On-premises network
Client VPN endpoint
Clients
Client CIDR range: 10.0.0.0/22

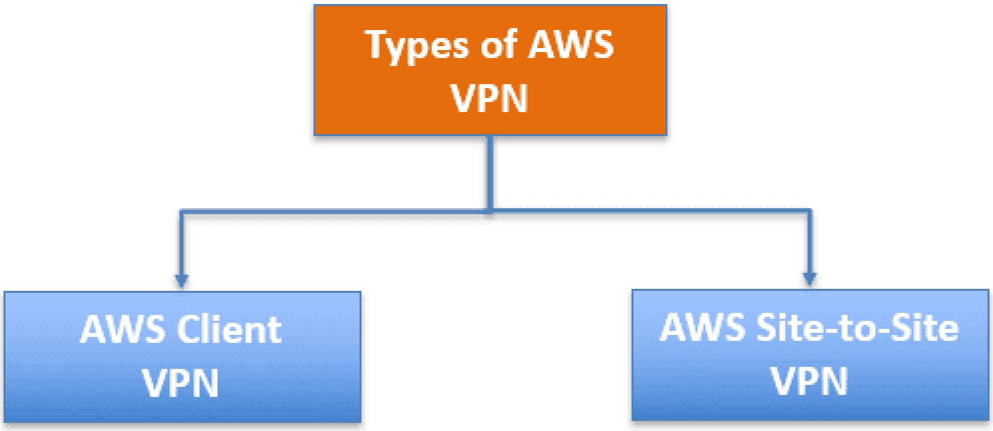
Components of AWS VPN



1. **Virtual Private Gateway – VGW**
   - A virtual private gateway is the VPN concentrator on the AWS side of the VPN connection
2. **Customer Gateway – CGW**
   - A customer gateway is a physical device or software application located on the customer side of the VPN connection.

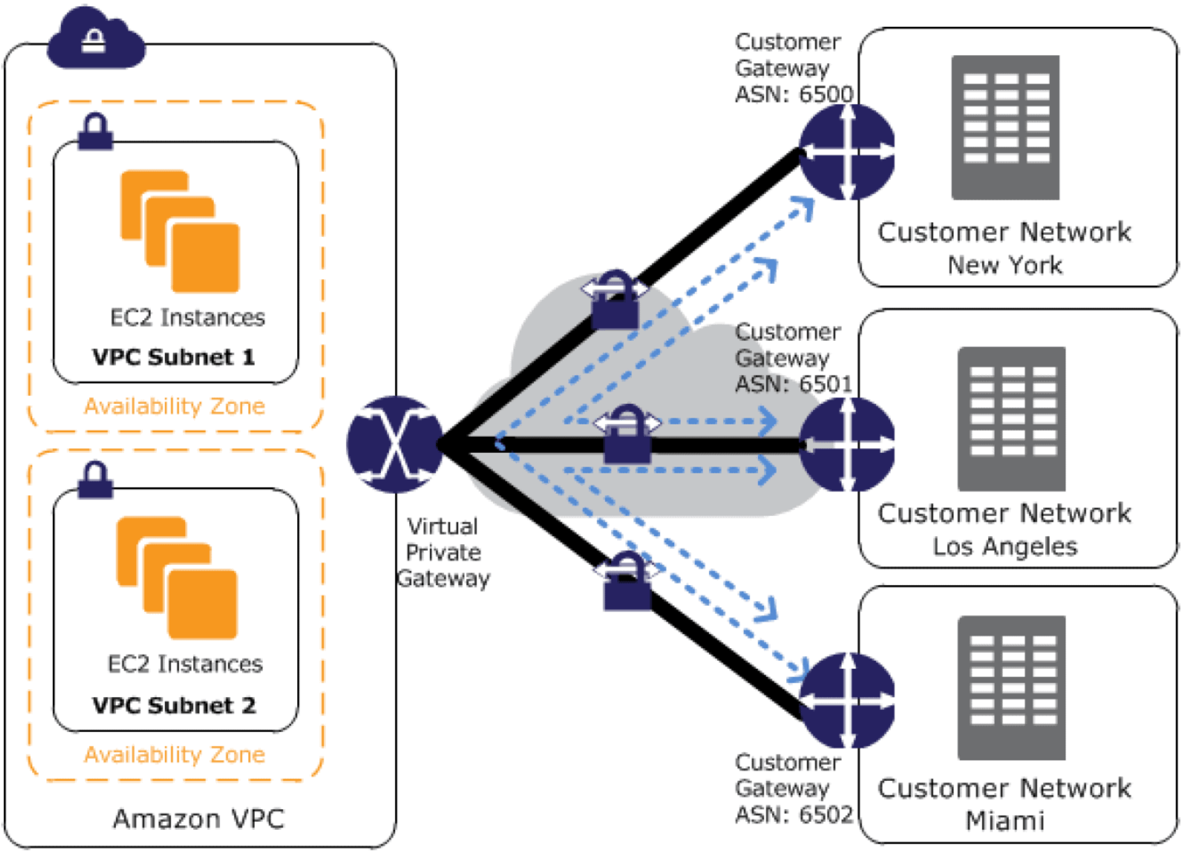
Types of AWS VPN

It provides **two private connectivity options** with the high availability and strong security your data needs:



VPN CloudHub

If you have multiple VPN connections, it can be used to provide secure communication between multiple on-premises sites. It uses a Virtual Private gateway in a detached mode that can be used without a VPC and operates on a simple hub-and-spoke model.


EC2 Instances
VPC Subnet 1
Availability Zone
EC2 Instances
VPC Subnet 2
Availability Zone
Amazon VPC
Virtual Private Gateway
Customer Gateway ASN: 6500
Customer Network
New York
Customer Gateway ASN: 6501
Customer Network
Los Angeles
Customer Gateway ASN: 6502
Customer Network
Miami