28. AWS Virtual Private

Cloud VPC

AWS Virtual Private Cloud (VPC) is a best example of **Infrastructure as a Service** (IaaS) on cloud computing, under Amazon VPC you will have benefit of using the scalable infrastructure.

Using AWS VPC you can create a virtual network in which it resembles a traditional network that your manager in your real and physical data center.

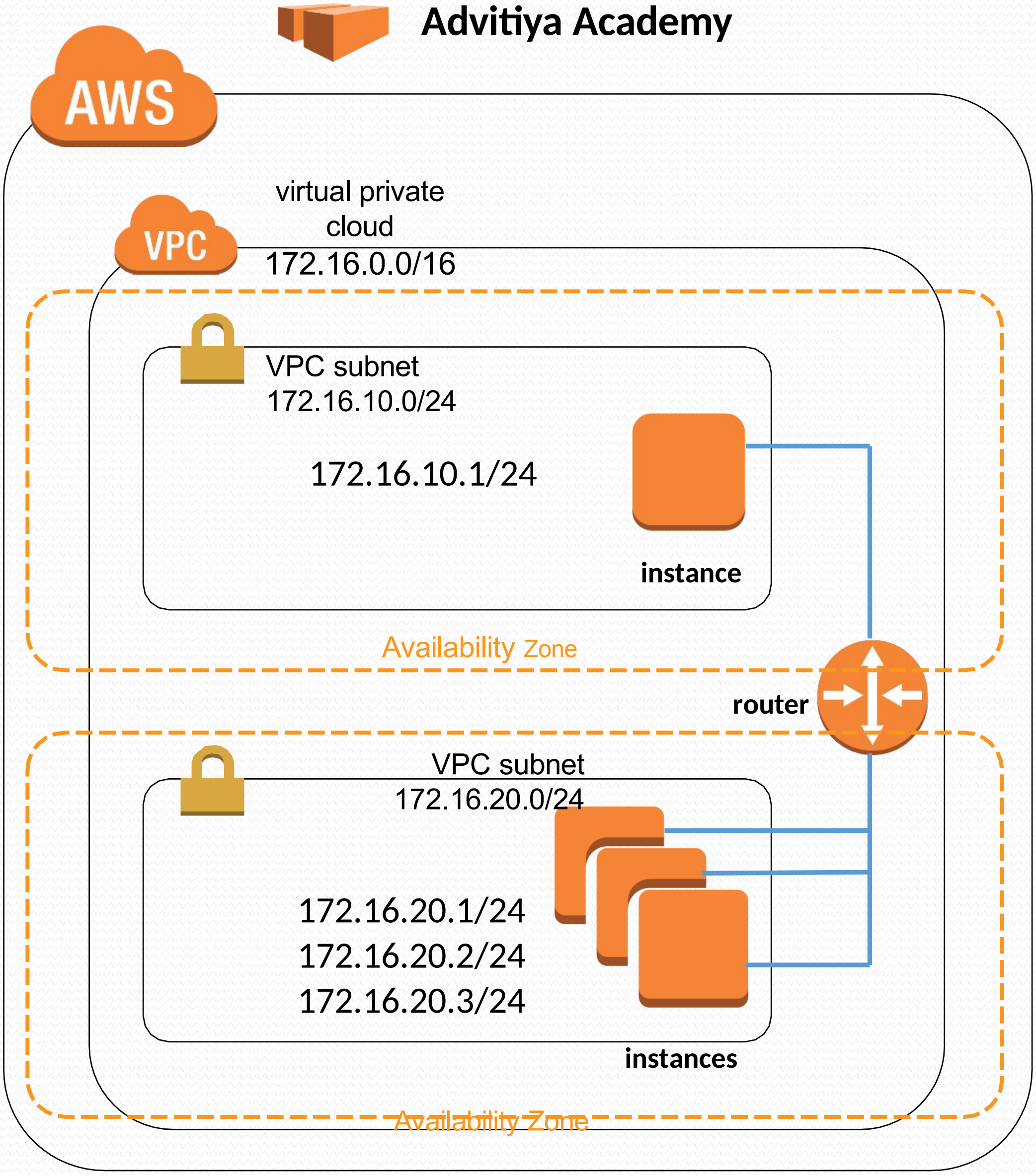
VPC is a logically isolated network in your account, you can create multiple virtual private network but all VPC are separate from each other.

AWS VPC contains almost every resource required to operate and manage a virtual network. For example: a VPC can contain subnets, EC2 Instances, Internet Gateways, route tables, DHCP options, Elastic IP addresses, NAT gateways, security options, VPN connectivity, etc.

In brief, VPC act like a networking layer for EC2 and it permits you to build your own infrastructure within AWS. Before creation of VPC, you should choose an IPv4 address range using Classless Inter-Domain Routing (CIDR) block like 10.0.0.0/16 or 172.16.0.0/16 or 192.168.0.0/24 etc. Once the VPC is created, changes in IP address range at later stage are not allowed. In VPC, IP address range support from slash notation /16 to /28, and allocated ranges should not be overlapped with any other network.

Figure is shown to understand an Amazon VPC, which includes a CIDR block IPv4 address 172.16.0.0/16 for VPC. Two subnets with different IPv4 address ranges 172.16.10.0/24 and 172.16.20.0/24, and these subnets are placed in different Availability Zones, and route tables are also used to specify local routes.

Amazon VPC
Advitiya Academy



AWS Virtual Private Cloud consists the following components:

Subnets

Route Tables

Security Groups

Network Access Control Lists (NACLs)

Internet Gateways

Egress Only Internet Gateways

DHCP Options Sets

Elastic IPs

Endpoints

NAT Gateways

VPC Peering Connections

VPN Connections

Subnets

In IPv4 scheme, subnet is segment of IP address range. If you create multiple subnet in a VPC, they can be treated as different broadcast domain. This way you can separate EC2 instances. In order to provide intercommunication among subnets, you may write route in route tables. In AWS VPC there is a limitation to use CIDR blocks, largest subnet of /16 and smallest of /28 can be used. For this course we are assuming that the candidate has knowledge of IPv4 and IPv6 in detail.

When you create infrastructure in AWS first you create a VPC, and within the VPC you can create subnets. Usually one AWS region can have minimum two Availability Zones (AZ). So this is your choice as per infrastructure requirement, which subnet can create in which AZ. Subnet exists within one AZ and it can't be shared between AZs. However, one AZ can have multiple subnets.

Subnets are categorized or classified in two different ways:

Public Subnet

Private Subnet

Private Subnet:

A subnet which is connected with a route-table and does not connect with Internet Gateway known as Private Subnet. Therefore, internet traffic does not reach directly to Private Subnet.

Public Subnet:

Public subnet is connected with route-table which further connected with Internet Gateway of VPC to provide internet access.

Important: Each AWS VPC contains one public subnet

Route Tables

In AWS environment, you use VPC to create infrastructure and within one VPC multiple subnet can exist. In order to provide communication between different subnets or internet traffic through internet gateway, you do require a route table.

As per AWS a route table contains a set of rules, which is responsible to direct traffic. Each VPC must have one route table, and each subnet must be associated with one route table only. A route table can be associated with multiple subnet at the same time, but one subnet cannot be associated with more than one route table.

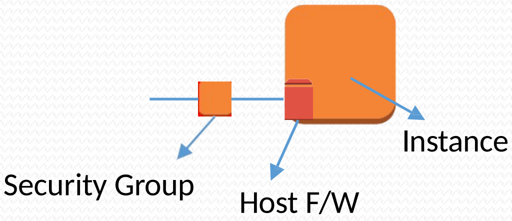
To understand about route table, we use an example,

For example, the following route table has a route for IPv4 Internet traffic (0.0.0.0/0) that points to an Internet gateway, and a route for 172.16.0.0/16 IPv4 traffic that points to a peering connection (pcx- 9o2b1w3b). Any traffic from the subnet that's destined for the 172.16.0.0/16 IP address range uses the peering connection, because this route is more specific than the route for Internet gateway. Any traffic destined for a target within the VPC (10.0.0.0/16) is covered by the Local route, and therefore routed within the VPC. All other traffic from the subnet uses the Internet gateway.

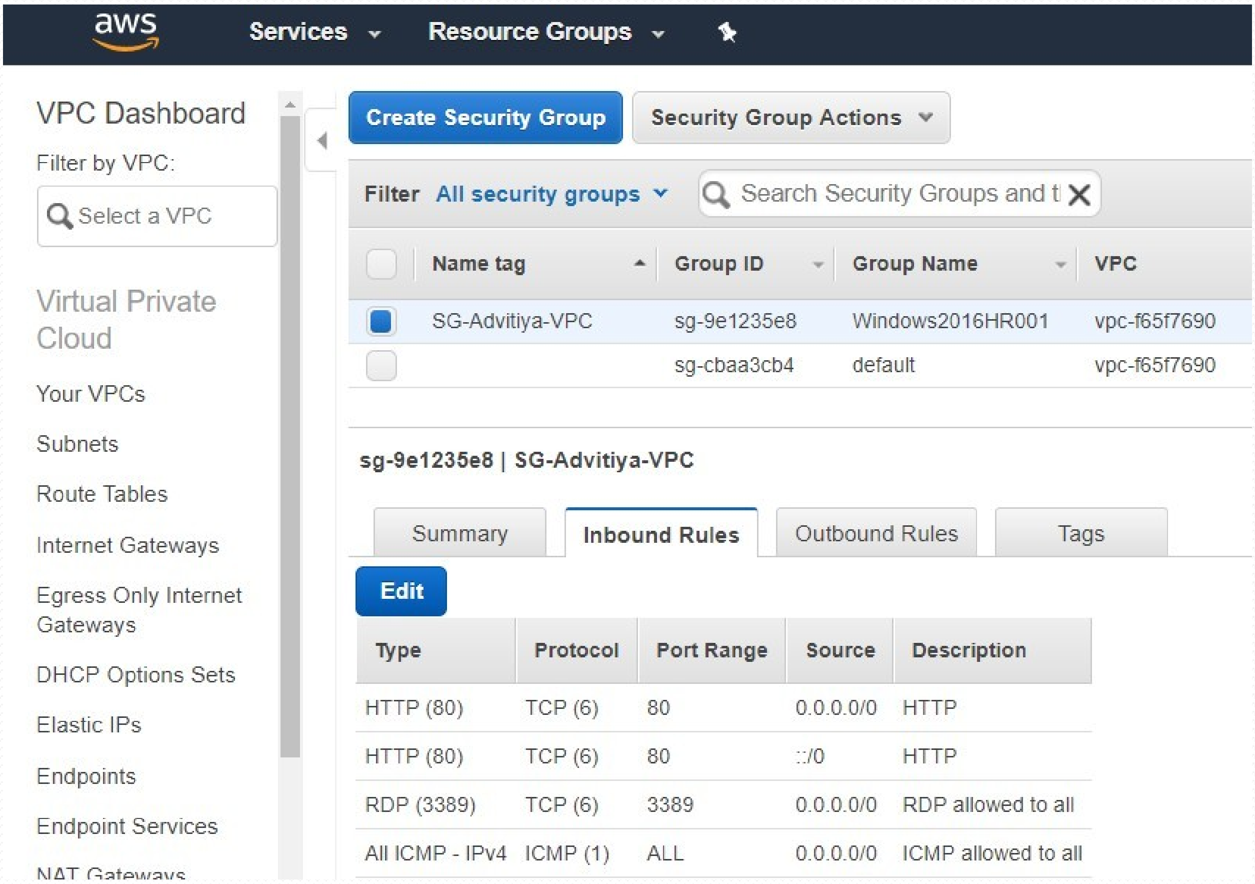
Destination	Target
10.0.0.0/16	Local
172.16.0.0/16	pcx-9o2b1w3b
0.0.0.0/0	igw-12bb32ab

Security Groups

A security group control inbound and outbound traffic for an instance within a VPC. A security group act as firewall for an instance.



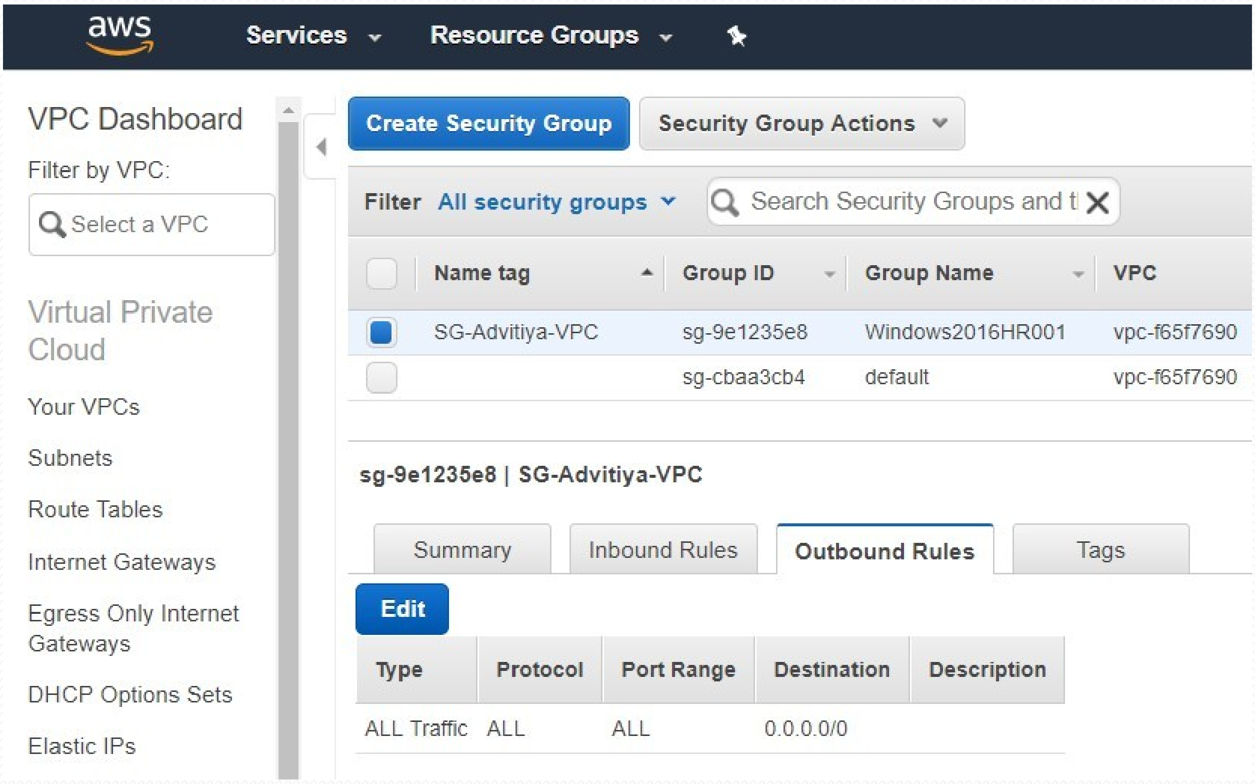
When you create an Instance in your VPC, maximum 5 security groups can be assigned to the instance. Security group can only work on Instance level. This is the reason, an instance in a subnet could be assigned to a different set of security groups.



□	Name tag	Group ID	Group Name	VPC
■	SG-Advitiya-VPC	sg-9e1235e8	Windows2016HR001	vpc-f65f7690
□		sg-cbaa3cb4	default	vpc-f65f7690

sg-9e1235e8 | SG-Advitiya-VPC

Type	Protocol	Port Range	Source	Description
HTTP (80)	TCP (6)	80	0.0.0.0/0	HTTP
HTTP (80)	TCP (6)	80	::/0	HTTP
RDP (3389)	TCP (6)	3389	0.0.0.0/0	RDP allowed to all
All ICMP - IPv4	ICMP (1)	ALL	0.0.0.0/0	ICMP allowed to all



	Name tag	Group ID	Group Name	VPC
☑	SG-Advitiya-VPC	sg-9e1235e8	Windows2016HR001	vpc-f65f7690
□		sg-cbaa3cb4	default	vpc-f65f7690

sg-9e1235e8 | SG-Advitiya-VPC

Type	Protocol	Port Range	Destination	Description
ALL Traffic	ALL	ALL	0.0.0.0/0	

The following are the significant characteristics of security groups:

In Security Groups, you can apply allow rules not deny rules.

In security groups, you have provision to configure Inbound and Outbound rules separately.

By default in security groups all outbound traffic is allowed. In order to specify outbound traffic you must delete the default rule and add outbound rules for specific port or service.

Security Groups are stateful, its mean your instance sends a request, and the response traffic related to the request service is allowed regardless of inbound rules.

Instances within a VPC associated with a common security group cannot speak to each other until you specify rules to allow communication.

Security Groups are also connected with Network Interfaces. After launching an EC2 Instance you can change or replace security groups any time associated with the instance, which changes the security groups connected with the primary network interface.

Network Access Control Lists (ACLs)

This is a second or another layer of security which works on subnet level, however security groups work on instance level. A network access control list works as a stateless firewall, therefor return traffic explicitly must have allowed rules. When you create a VPC, by default a network access control list (ACL) is associated with every subnet and allows all inbound and outbound traffic.

For ACL recommendation, use the below link.

https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Appendix_NACLs.html

Internet Gateways

Internet Gateway provides communication between your VPC's instances and the Internet. It is by default scaled, highly available and redundant. Usually you attach an Internet Gateway with a subnet which allows the Internet traffic to Instances within the subnet.

Egress Only Internet Gateways

An egress only internet gateway allows outbound communication over IPv6 from an EC2 Instance to the Internet.

Any instance which is running in a public subnet and configured with IPv4 can connect to internet gateway in order to provide internet traffic over the instance. The same way you would require Egress Only Internet Gateway to provide the Internet traffic over IPv6 configured EC2 Instance.

DHCP Options Sets

Dynamic Host Configuration Protocol (DHCP) is used to distribute IP addresses to networked nodes using a range of IP addresses. But here DHCP provides a standard for passing configuration parameters to hosts such as domain name, dns and netbios-node-type. By default DHCP options sets are linked with your virtual private clouds (VPC).

Elastic IPs

Elastic IP Address (EIP) is a static public IP address. You can allocate an EIP from the range to resource within the VPC and can release it if not required. Amazon does charge for allocated EIP address, even when those EIPs are not associated with resource.

Endpoints

A VPC endpoint allows you to securely connect your VPC to another service.

A VPC endpoint enables you to create a private connection between your VPC and another AWS service without requiring access over the Internet, through a NAT device, a VPN connection, or AWS Direct Connect. Endpoints are free of charge.

In a VPC, endpoints allow EC2 Instances to communicate with resources in other services of AWS. In brief your instance does not require public IP address, Internet Gateway, NAT device or a virtual private gateway in your VPC. You only require endpoint policy to control access to resource in other AWS services.

Important:

https://www.cloudberrylab.com/blog/creating-and-accessing-amazon-s3-vpc-endpoint/

https://aws.amazon.com/blogs/aws/new-vpc-endpoint-for-amazon-s3/

NAT Gateways

In order to provide the Internet in private subnet you can use a Network address translation (NAT) gateway. NAT gateways support to IPv4 and do not support to IPv6 network traffic. NAT gateways in AWS environment behaves like a NAT instance which is easy to manage and by default highly available.

AWS charges for NAT gateway creation on hourly usage basis. AWS also charges for data transfer from EC2 instance. If you need to know about NAT gateway charges, simply refer the below table:

Region	Price per NAT gateway ($/hour)	Price per GB data processed ($)
US East (N. Virginia)	0.045	0.045
US East (Ohio)	0.045	0.045
US West (Oregon)	0.045	0.045
US West (N. California)	0.048	0.048
Canada (Central)	0.050	0.050
EU (Ireland)	0.048	0.048
EU (London)	0.050	0.050
EU (Paris)	0.050	0.050
EU (Frankfurt)	0.052	0.052
Asia Pacific (Singapore)	0.059	0.059

Asia Pacific (Tokyo)	0.062	0.062
Asia Pacific (Seoul)	0.059	0.059
Asia Pacific (Sydney)	0.059	0.059
Asia Pacific (Mumbai)	0.056	0.056
South America (São Paulo)	0.093	0.093
AWS GovCloud (US)	0.054	0.054

Note: For more detail related to price you can browse **Amazon VPC pricing** page.

Important: Before start configuring NAT gateway, ensure in your AWS account that the Internet Gateway is attached with the VPC.

To configure NAT gateways, follow these simple steps:

- In first step, route table must be associated with private subnet to direct Inbound traffic to the NAT gateway.
- The NAT gateway must be associated with an Elastic IP address (EIP).

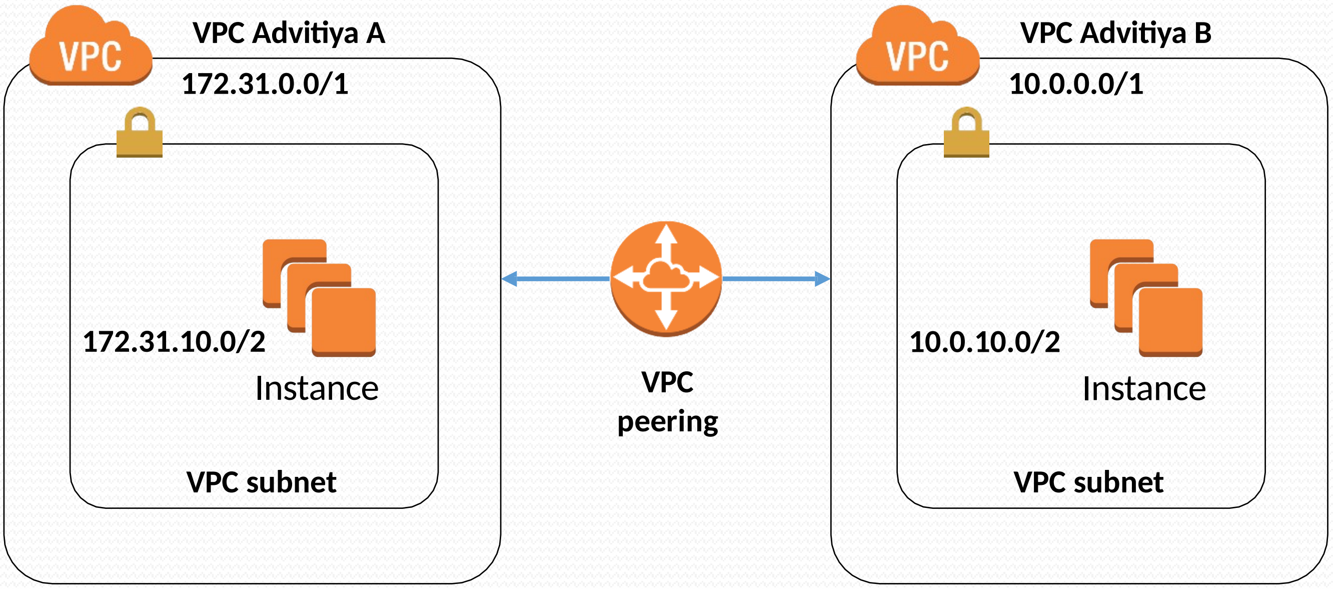
VPC Peering Connections

If you are working with multiple VPC in your account and you want to make connection between them. VPC Peering will provide connectivity between two VPCs.

A VPC peering connection is a network connection which enables network traffic between two VPCs using private IP addresses or IPv6 addresses.

You can also create VPC peering between VPCs belong to different accounts or accounts in different regions.

The following figure will give better picture to understand VPC peering:



(VPC Peering)

Virtual Private Network (VPN) Connections

In a generic term, VPN is a technology through by which you can connect two remote network using some encapsulation for secure data transfer. Popular protocols to configure VPN are:

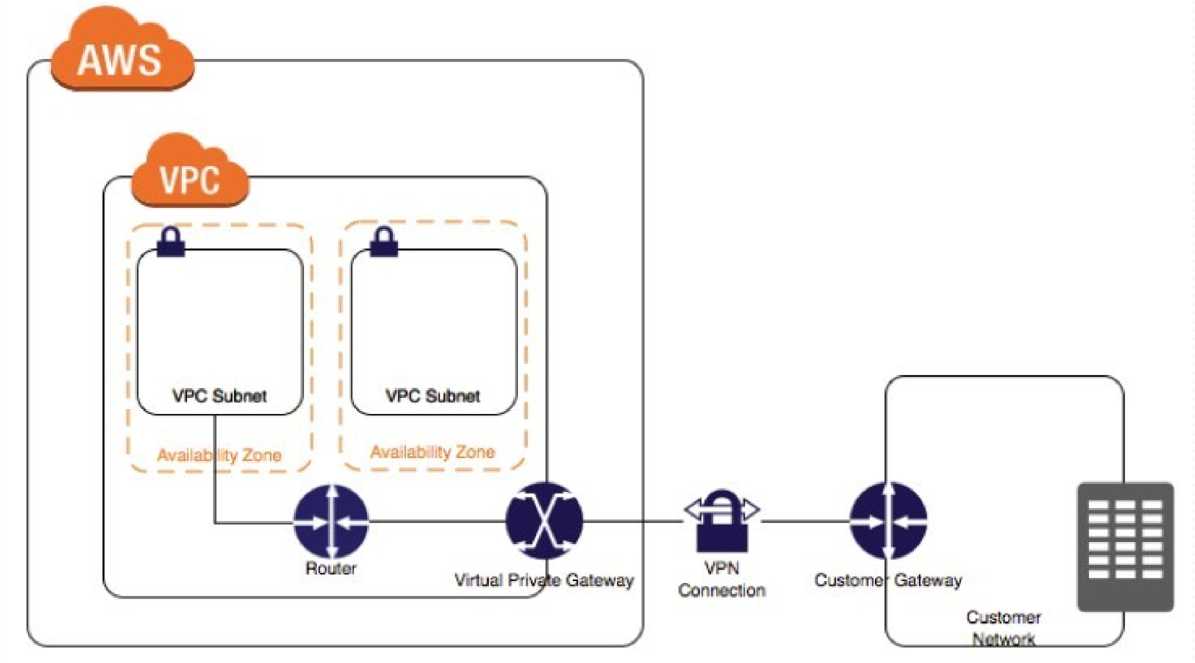
Internet Protocol Security (IPSec)

Layer to Tunneling Protocol (L2TP)

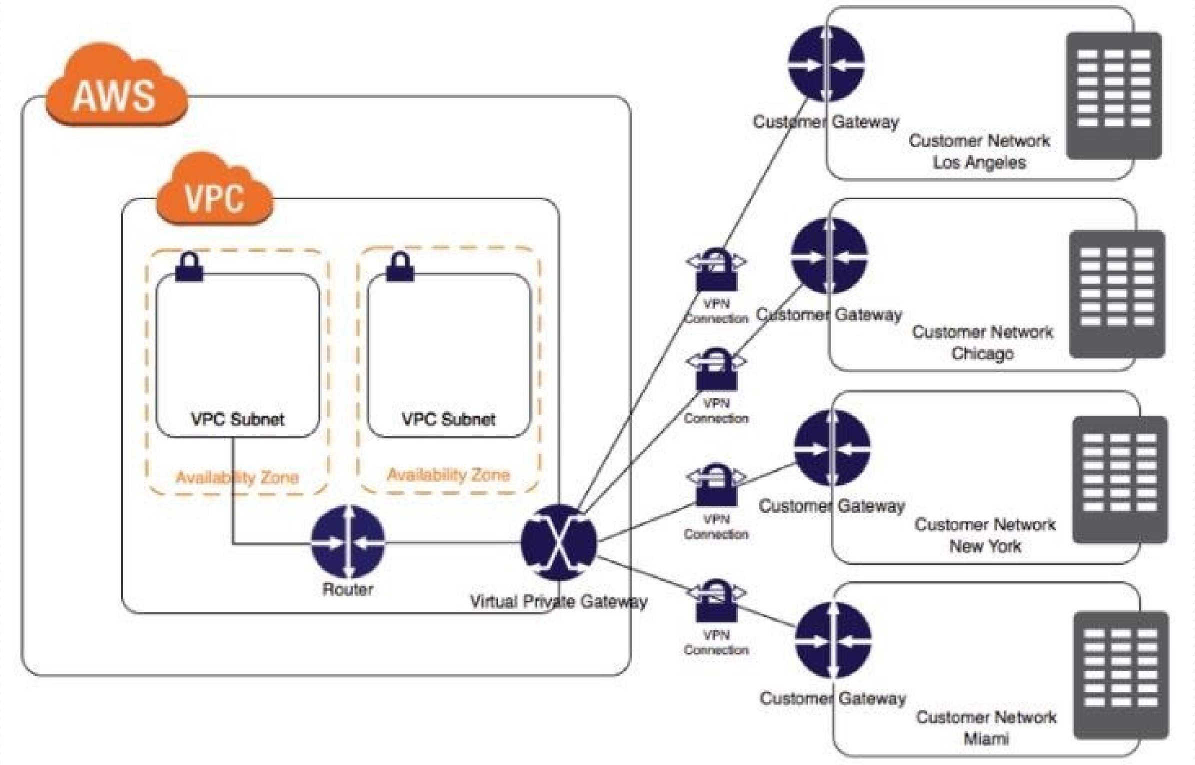
Point to Point Tunneling Protocol
(PPTP)

AWS VPN allows to make connection between your AWS VPC and your own network by using IPSec VPN connections. AWS only does support to IPv4 traffic through a VPN connection.

Single and multiple VPN connection example diagrams:



(Single VPN Connection)



(Multiple VPN Connection)