VPC (virtual private cloud)

1. Virtual private cloud is a virtual network that closely resembles traditional networking that you operate in your own data center, with the benefits of using the scalable infrastructure of AWS.
2. It is logically isolated from other virtual network in the AWS cloud.
3. Maximum 5 VPC can be created and 200 subnet & 200 route table in each VPC.
4. We can allocate maximum 5 elastic IP.
5. Once we created VPC, Route table & NACL will be automatically created.
6. A VPC is confined to an AWS region and does not Extend between region.
7. The different subnet within a VPC cannot overlap.
8. VPC created in region not in AZ.
9. Subnet created in AZ not in region.
10. When you create a VPC you must specify an IPv4 CIDR block for the VPC. The allowed block size is between /16 to /28 .

11. The first four & last IP address of subnet cannot be assigned because reserved for AWS.

a. First IP for Network Address

b. Second IP for VPC route.

c. Third IP for DNS server

d. Fourth IP for Future use.

e. Last IP of each subnet for Broadcast IP.

Aws does not support broadcast in a VPC but reserve this address.

VPC types

Default VPC- created in each AWS region when an AWS account is created.

Default CIDR, security group, NACL and route table setting.

Internet Gateway by default attached to VPC.

Custom VPC- VPC on AWS account owner Creates.

IGW by default not created and not attached to VPC.

Public subnet- if subnet traffic is routed to an internet Gateway the subnet is known as public subnet. If you want your instance in a public subnet to communicate with the internet over IPv4, it must have public IPv4 or an Elastic IP address.

Private subnet- if a subnet does not have a route to the internet gateway, the subnet is known as private subnet.

IGW- an IGW is virtual router that connects VPC to the internet.

If you create a new VPC then you must attach the IGW in order to access the internet.

Route Table- A route table contains a set of rules, called routes , that are used to determine where network traffic from your subnet or gateway is directed.

It connects the different AZ together and connects the VPC to the IGW.

You can have up to 200 route tables per VPC

You can have up to 50 routes entries per route table

Each subnet must be associated with only one route table at any given time

If you do not specify a subnet to route then subnet will be associated with the default VPC route table.

NAT Gateway- you can use NAT gateway to enable instances in a private subnet to connect to the internet or other AWS service, but prevent the internet from initiating a connection with those instances.

You are charged for creating and using a NAT Gateway in your account. NAT Gateway charges hourly usage & data processing & EC2 charges for data transfer also apply.

Security Group-

It is a virtual firewall works at ENI level (elastic network interface)

Up to 5 security groups per EC2 instance can be applied.

You can only have permit rules cannot have deny rule.

In security group when you allow inbound rules then outbound rule automatic allow so it called stateful.

NACL- is an optional layer of security for your VPC that acts as a firewall for controlling traffic in & out of one or more subnets.

You can create a custom NACL & associate it with a subnet. By default each custom NACL denies all inbound & outbound traffic until you add rules.

You can associate NACL with multiple subnets however subnet can be associated with only one NACL at a time when you associate NACL with a subnet the previous association is removed.

It functions at the subnet level.

NACL are stateless, outbound traffic also allow for inbound traffic here.

You can have permit & deny rules in a NACL.

What is VPC peering?

A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 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. The VPCs can be in different regions (also known as an inter-region VPC peering connection).

A VPC peering connection helps you to facilitate the transfer of data. For example, if you have more than one AWS account, you can peer the VPCs across those accounts to create a file sharing network. You can also use a VPC peering connection to allow other VPCs to access resources you have in one of your VPCs.

You can establish peering relationships between VPCs across different AWS Regions (also called inter-Region VPC peering). This allows VPC resources including EC2 instances, Amazon RDS databases and Lambda functions that run in different AWS Regions to communicate with each other using private IP addresses, without requiring gateways, VPN connections, or separate network appliances. The traffic remains in the private IP space. All inter-region traffic is encrypted with no single point of failure, or bandwidth bottleneck.

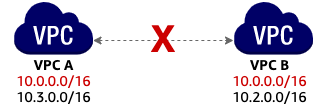
To establish a VPC peering connection, you do the following:

1. The owner of the requester VPC sends a request to the owner of the accepter VPC to create the VPC peering connection. The accepter VPC can be owned by you, or another AWS account, and cannot have a CIDR block that overlaps with the CIDR block of the requester VPC.
2. The owner of the accepter VPC accepts the VPC peering connection request to activate the VPC peering connection.
3. To enable the flow of traffic between the VPCs using private IP addresses, the owner of each VPC in the VPC peering connection must manually add a route to one or more of their VPC route tables that points to the IP address range of the other VPC (the peer VPC).
4. If required, update the security group rules that are associated with your instance to ensure that traffic to and from the peer VPC is not restricted. If both VPCs are in the same region, you can reference a security group from the peer VPC as a source or destination for ingress or egress rules in your security group rules.
5. With the default VPC peering connection options, if EC2 instances on either side of a VPC peering connection address each other using a public DNS hostname, the hostname resolves to the public IP address of the instance. To change this behavior, enable DNS hostname resolution for your VPC connection. After enabling DNS hostname resolution, if instances on either side of the VPC peering connection address each other using a public DNS hostname, the hostname resolves to the private IP address of the instance.

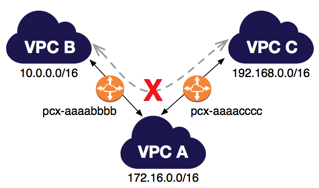
Unsupported VPC peering configurations

1. Overlapping CIDR blocks- You cannot create a VPC peering connection between VPCs with matching or overlapping IPv4 CIDR blocks.





Transitive peering -You have a VPC peering connection between VPC A and VPC B (pcx-aaaabbbb), and between VPC A and VPC C (pcx-aaaacccc). There is no VPC peering connection between VPC B and VPC C. You cannot route packets directly from VPC B to VPC C through VPC A. To route packets directly between VPC B and VPC C, you can create a separate VPC peering connection between them (provided they do not have overlapping CIDR blocks)



Example: Edge to edge routing through a VPN connection or an AWS Direct Connect connection

You have a VPC peering connection between VPC A and VPC B. VPC A also has a Site-to-Site VPN connection or an AWS Direct Connect connection to a corporate network. Edge to edge routing is not supported; you cannot use VPC A to extend the peering relationship to exist between VPC B and the corporate network. For example, traffic from the corporate network can’t directly access VPC B by using the VPN connection or the AWS Direct Connect connection to VPC A.

