**VPC**

**What is VPC…?**

* VPC stands for virtual private cloud.
* VPC is a service offered by AWS that allows users to launch AWS resources into an isolated networks on the cloud. With VPC users can create and manage virtual networks having their own IP addresses, subnets, routing tables, enables them to launch AWS resources.
* VPC configuration involves management of virtualized components of AWS resources in your account. The resources of subnets, security groups, NACL, routing table.

**What is CIDR…?**

* CIDR stands for classless inter domain routing. CIDR is used to allocating the IP address over the internet. CIDR improves data routing efficiency on the internet.
* CIDR is used by organization to allocation IP addresses efficiently and flexibility.
* Benefits of CIDR:
* Reduces IP address wastage.
* Transmits data quickly.
* Create the VPC.
* Create subnet flexibly.
* CIDR allows network routers to route data packets to the respective routers based on there subnets.
* CIDR blocks is a collection of IP address consist of same networks prefix and number of bits.
* CIDR notation represents an IP address and suffix that indicates network identifier bits in specified format.

**Subnetting:**

* Subnet is a range of IP addresses in your VPC. Each subnet must be reside in one availability zone and it cannot be associated in more than one availability zone. If subnets can be launched in more than one availability zone if one zone application failure it will be shifted to another zone.

**Subnet IP address range:**

* **IPV4 only:** The subnet has an IPV4 CIDR block does not have any IPV6 CIDR block. Resources in an IPV4 block communicates only with IPV4.
* **Dual stack:** The subnet has both IPV4 and IPv6 CIDR block. Resources in Dual stack subnet communicate over IPV4 and IPV6.
* **IPV6 only:** The subnet has an IPV6 CIDR block does not have any IPV4 CIDR block. Resources in an IPV6 block communicates only with IPV6.

**Subnet Types:**

* **Public Subnet:** The subnet has a direct route to the Internet gateway.
* **Private Subnet:** The subnet does not have direct route to the Internet gateway.
* **Isolated Subnet:** The subnet does not have routes to destination outside of VPC.
* **VPN Subnet:** The subnet have route to site-to-site VPN connection through a virtual private gateway.

**Subnet Routing:**

* Each subnet must be associated with a route table, which specifies the allowed routes for outbound traffic leaving subnet.

**Security Groups:**

* A security group that control the traffic which is allowed to reach and leave the resource that is associated with it. Security group which acts as the virtual firewall.
* When you create a VPC then a security group is created defaultly. You can create additional groups with a VPC, each with their own inbound rules and outbound rules.
* Inbound rules contain source, port range, protocol for each inbound rule. Outbound rules contain destination, port range, protocol for each outbound rules.
* You can assign a security group to your resource then VPC of both security group which is created and resource’s VPC is need to be same.
* You can associate multiple security groups to a single resource, the rules which are associated to all the security groups are associated to the resources. You can add, delete, or update the rules which are associated.
* Rules of creating a Security group:

1. A security group must contain VPC.
2. Name and description of the security group is need to be up to 255 character.
3. The characters are need to be [A-Z][a-z][0-9],spaces and !@#$%^&\* etc. are used.
4. When the name contains trailing spaces, the space at the end of name is trimmed.
5. A security group cannot be start with “sg“.

* Components of security group rule:

1. **Protocol:** The protocol that allows. The commonly used protocols are TCP, UDP, SSH, and ICMP.
2. **Port range:** The range of ports that allows traffic. You can specify single port number or range of port numbers.
3. **ICMP type and code:** Internet control message protocol (ICMP) it is network layer protocol which is used to error-reporting, host discovery, and source routing.
4. **Source and destination:** source means inbound rules and destination means outbound rules.

**NACL (Network Access Control List):**

* NACL allows or denies the inbound or outbound traffic at subnet level. You can use the default network ACL for your VPC or you can create a new custom NACL. While creating the custom NACL we will add similar rules which we added at the security groups.
* A VPC must comes with the modifiable default NACL. By default, it allows all the inbound and outbound IPV4 traffic.
* You can create a custom VPC associated with subnet which allows or denies specific inbound or outbound traffic at subnet level.
* Each subnet is need to be associated with a NACL it can be default or custom. If it is not associated with the custom NACL it will be associated with the default NACL.
* You can associate one NACL to the multiple subnet, but vice versa is not possible. When a NACL is associated with the subnet, if you associate a new on the old one with disassociated.
* NACL are stateless means the information which is sent or received previously will not be stored. Where security groups are stateful.
* **Parts of NACL rules:**
* **Rules:** Rules are evaluated starting with the lowest numbered rules.
* **Type:** The Type of traffic. You can also specify all traffic or custom range.
* **Protocol:** You can specify any protocol that has a standard protocol number.
* **Port range:** Listening port or port ranges for traffic.
* **Source:** The source of traffic.
* **Destination:** The destination of traffic.
* **Allow/Deny:** Whether to allow or deny the traffic.

**VPC Peering:**

* VPC peering is network connection between two VPCs that enables you to traffic between them using private IPV4 or IPV6.
* VPCs can communicate in the same network. To communicate the VPC in the two different account you need to use VPC peering. It neither needs gateway nor VPN connection, does not rely on the physical hardware. In the communication it will not face any failure.
* VPCs that are in the two different account or region they need to they communicate with private IPs, without any gateways, network appliances, or VPN connections.

**NAT Gateway:**

* You can use the NAT Gateway so that instances in the private subnet can connect to services outside of the VPC, But the external services cannot get the unsolicited connection with private subnet.
* **Public:** Instances in the private subnet can connect to the internet through a public NAT gateway but cannot receive the unsolicited connection inbound connection from the internet. We can associate the elastic IP address.
* **Private:** Instances in the private subnet can connect to other VPCs through private NAT gateways. You can route traffic from the NAT gateway through transmit gateway or virtual private gateways. No elastic IP address are used.
* NAT gateway is created in every specialized zone with redundancy. There will be a quota of number of NAT gateways can be created in the each availability zone.
* If you create the single NAT gateway for all the availability zone, If the NAT gateway is down then the internet connection will be lost in all the availability zones.
* NAT gateway uses TCP, UDP, ICMP.
* NAT gateway are supported for IPV4 or IPV6. For IPV6 traffic, it performs NAT64 by using conjunction with DNS64. A NAT gateway can support 5GB bandwidth and automatically scales up to 100GB. To require more bandwidth you need to create the multiple NAT gateways for the multiple network.
* NAT gateways can process up to one million packets per second and automatically scales up to ten million packets per second. To reduce the packet loss for multiple subnet you need to create a separate NAT gateway.
* Each IPV4 address can support up to 55,000 unique destinations simultaneously. The unique destination is identified by unique combinations of destination port, destination IP address, protocol. You can increase the limit associating up to 8 IPV4 address to your NAT gateway( 1 primary IPV4 and 7 secondary IPV4). Your limited to associated up to 2 elastic IP addresses.
* You cannot associate security groups with NAT gateway. It uses port from 1024 to 65535.
* By default the user does not have permission to work with a NAT gateway. You can create a IAM role with policy attached that grants users permissions to create, describe or delete NAT gateways.

**VPC Endpoints:**

* A VPC endpoint enables customers to privately connect to supported AWS service and VPC endpoints powered by Amazon private link. VPC Endpoints does not require any public IP address.
* It enables the communication between instances in an Amazon VPC and services without imposing availability risks.
* There two types of VPC:
* Interface endpoints.
* Gateway endpoints

**VPC Flow Logs:**

* Flow log is a feature that enables you to capture information about IP traffic going to and from in network interface with in your VPC. Flow logs does not disturb network latency or through put.
* Flow log records Types:
* **Aggregation interval:** It is a period of time during which particular flow is captured and aggregated it into the flow logs. The maximum aggregation time is 10 minutes, When you create a flow log the maximum aggregation time which is given is 1 minutes.
* **Default Format:** With the default format, the flow log records include the version 2 fields.
* **Custom Format:** With custom format, you specify the which field are included in the flow log record in which order.

**VPN Connection:**

* A VPN (Virtual Private Network) connection in AWS (Amazon Web Services) allows you to securely connect your on-premises network to the AWS network.
* This can be useful for accessing AWS resources, such as EC2 instances, RDS databases, and S3 buckets, from your local network. To set up a VPN connection in AWS, you will need to configure an AWS VPN gateway, create a VPN client on your local network, and connect the two networks using the VPN client.
* You will also need to configure security options, such as IPsec encryption, to ensure the security of your VPN connection. AWS provides documentation and tools to help you set up and manage VPN .