1. Difference between NACL & Security Group

Ans:- Here is a summary of the main differences between AWS Network Access Control Lists (NACLs) and Security Groups:

● Layer of defense: NACLs operate at the subnet level and control traffic in and out of a VPC, while Security Groups operate at the instance level and control traffic to and from individual EC2 instances.

● Scope of application: NACLs apply to all instances in a subnet, while Security Groups apply to individual instances.

● Statefulness: NACLs are stateless and do not track the state of a connection, while Security Groups are stateful and allow traffic based on the response to previous traffic.

● Default rule: NACLs have a default rule that denies all traffic, while Security Groups have a default rule that allows all traffic.

● Order of rules: NACLs have a numbered list of rules that are applied in order, while Security Groups do not have an order of rules.

● Ability to block traffic: NACLs can block traffic at the subnet level, while Security Groups can only block traffic at the instance level.

● Network performance: NACLs can potentially have a larger impact on network performance because they operate at the subnet level and apply to all instances in the subnet, while Security Groups only operate at the instance level and only apply to individual instances.

2. What is NAT Gateway?

Ans: A Network Address Translation (NAT) gateway in Amazon Web Services (AWS) is a highly available, managed network component that enables instances in a private subnet to connect to the internet or other AWS services, but prevents the internet from initiating connections with those instances. NAT gateways are used to provide outbound-only internet connectivity for instances in private subnets, which do not have public IP addresses or Elastic IP addresses.

3. What is NAT Instances?

Ans:A NAT instance provides network address translation (NAT). You can use a NAT instance to allow resources in a private subnet to communicate with destinations outside the virtual private cloud (VPC), such as the internet or an on-premises network.

4. What is VPC Peering Connection?

Ans: 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.

5. What is VPCs Endpoint?

Ans: "A VPC endpoint enables customers to privately connect to supported AWS services and VPC endpoint services powered by AWS PrivateLink". Amazon VPC instances do not require public IP addresses to communicate with resources of the service. Traffic between an Amazon VPC and a service does not leave the Amazon network.

6. When do you use VPCs Endpoint?
Ans:Vpc endpoints is a simple infrastructure architecture. "You can use an interface endpoint to connect traffic from an instance to a service such as SQS(message queuing service), or you can: Configure an internet gateway. Configure security group or network ACL rules.

7. What is Vpn?
Ans: VPN stands for "Virtual Private Network" and describes the opportunity to establish a protected network connection when using public networks. VPNs encrypt your internet traffic and disguise your online identity. This makes it more difficult for third parties to track your activities online and steal data.

8. What is Aws Vpn connection/servicess?
Ans: AWS VPN is a service that allows you to establish a secure, private connection between your on-premises data center and your VPCs. It uses the Internet Protocol Security (IPSec) protocol to encrypt data and establish a secure connection, and can be used with both static and dynamic routing.
AWS VPN is a fully managed service, and is easy to set up and use. To use AWS VPN, you will need to create a VPN connection and configure it to connect to your VPCs. You will also need to create a customer gateway and a virtual private gateway, and configure them to connect to your on-premises network.

9. What is Transit Gateway? Where to be user it?
Ans:Amazon Web Services (AWS) Transit Gateway is a network transit hub that enables you to connect your Amazon Virtual Private Clouds (VPCs) and on-premises networks to a single gateway. It simplifies the process of connecting multiple VPCs and on-premises networks by allowing you to manage all of your connections through a single, centralized interface.

10. What is Aws Direct connect? where to be use it?
Ans: AWS Direct Connect is a network service that allows you to establish a dedicated connection between your on-premises data centres and AWS. This connection bypasses the public internet and provides a more reliable and secure way to transfer data between your on-premises and cloud resources.

To use AWS Direct Connect, you will need to order a Direct Connect circuit and connect it to your on-premises network. You can then use the Direct Connect console or the Direct Connect API to create virtual interfaces and link them to your VPCs or other AWS resources.
AWS Direct Connect is a cost-effective solution for transferring large amounts of data between your on-premises and cloud resources. It is also a good choice if you have strict security or compliance requirements, or if you need to transfer data with low latency.

11. what is the OSI model? what is OSI 7 Layers?
Ans: The Open Systems Interconnection (OSI) model describes seven layers that computer systems use to communicate over a network.
The seven layers of the model are given next:

Physical layer
The physical layer refers to the physical communication medium and the technologies to transmit data across that medium. At its core, data communication is the transfer of digital and electronic signals through various physical channels like fiber-optic cables, copper cabling, and air. The physical layer includes standards for technologies and metrics closely related with the channels, such as Bluetooth, NFC, and data transmission speeds.

Data link layer
The data link layer refers to the technologies used to connect two machines across a network where the physical layer already exists. It manages data frames, which are digital signals encapsulated into data packets. Flow control and error control of data are often key focuses of the data link layer. Ethernet is an example of a standard at this level. The data link layer is often split into two sub-layers: the Media Access Control (MAC) layer and Logical Link Control (LLC) layer.

Network layer
The network layer is concerned with concepts such as routing, forwarding, and addressing across a dispersed network or multiple connected networks of nodes or machines. The network layer may also manage flow control. Across the internet, the Internet Protocol v4 (IPv4) and IPv6 are used as the main network layer protocols.

Transport layer
The primary focus of the transport layer is to ensure that data packets arrive in the right order, without losses or errors, or can be seamlessly recovered if required. Flow control, along with error control, is often a focus at the transport layer. At this layer, commonly used protocols include the Transmission Control Protocol (TCP), a near-lossless connection-based protocol, and the User Datagram Protocol (UDP), a lossy connectionless protocol. TCP is commonly used where all data must be intact (e.g. file share), whereas UDP is used when retaining all packets is less critical (e.g. video streaming).

Session layer
The session layer is responsible for network coordination between two separate applications in a session. A session manages the beginning and ending of a one-to-one application connection and synchronization conflicts. Network File System (NFS) and Server Message Block (SMB) are commonly used protocols at the session layer.

Presentation layer
The presentation layer is primarily concerned with the syntax of the data itself for applications to send and consume. For example, Hypertext Markup Language (HTML), JavaScipt Object Notation (JSON), and Comma Separated Values (CSV) are all modeling languages to describe the structure of data at the presentation layer.

Application layer
The application layer is concerned with the specific type of application itself and its standardized communication methods. For example, browsers can communicate using HyperText Transfer Protocol Secure (HTTPS), and HTTP and email clients can communicate using POP3 (Post Office Protocol version 3) and SMTP (Simple Mail Transfer Protocol).

Not all systems that use the OSI model implement every layer.

12. Why we store ssh key (pem key) in Aws secrets manager? use cases.
Ans:Aws Secrets Manager helps you improve your security posture, because you no longer need hard-coded credentials in application source code.

Secret Manager works well for storing configuration information such as database passwords, API keys, or TLS certificates needed by an application at runtime. A key management system, such as Cloud KMS, lets you manage cryptographic keys and to use them to encrypt or decrypt data.