Right network setup for RDS and bastion host

What is an AWS Private Subnet?

On AWS, a subnet is a range of IP addresses within a virtual private cloud (VPC). A private subnet is a subdivision of a VPC that does not have direct connectivity to the public internet. It is designed to isolate resources and ensure that they are not directly exposed to potential threats from the external network.

AWS private subnets offer a powerful mechanism for ensuring compliance and enhancing security within cloud environments. By isolating resources from the public internet, organizations can protect sensitive data, meet regulatory requirements, and mitigate the risk of external threats.

Importance of Compliance

Compliance with industry regulations and data protection standards is a critical concern for businesses operating in various sectors. Here are some reasons why private subnets play a vital role in achieving compliance:

- Data Privacy and Confidentiality: Private subnets provide an additional layer of protection for sensitive data and resources. By segregating them from the public internet, organizations can better control access and minimize the risk of unauthorized exposure or data breaches.

- Regulatory Compliance: Many industries, such as healthcare (HIPAA), finance (PCI DSS), and government (FedRAMP), have specific regulations governing the handling and transmission of data. Private subnets help meet these compliance requirements by enforcing strict access controls, logging, and monitoring mechanisms.

- Secure Communication Channels: Private subnets enable secure communication between resources within the same VPC. By leveraging private IP addresses and internal routing, organizations can establish private connections without relying on the internet, mitigating the risk of interception or eavesdropping.

- Protection Against External Threats: By placing resources in private subnets, organizations limit their exposure to the public internet and reduce the attack surface. This isolation minimizes the potential impact of external threats, such as distributed denial-of-service (DDoS) attacks, network scanning, or unauthorized access attempts.

Example of how an EC2 instance in a private subnet can be accessed by a public user using an Application Load Balancer (ALB):

Let's assume you have set up a VPC with a public subnet and a private subnet. In the private subnet, you have an EC2 instance hosting your application, and in the public subnet, you have an ALB.

- To enable public user access to the application, you configure the ALB to listen on a specific port (e.g., port 80 for HTTP). You create a target group and add the private EC2 instance as its target. Next, you configure the security group of the private EC2 instance to allow incoming traffic from the ALB's security group on the specified port. Optionally, you can restrict access to the EC2 instance by allowing traffic only from the ALB's security group.

- To make the application accessible to the public, you associate a domain name with the ALB using Route 53 or any other DNS service. This allows the public user to access the application by simply accessing the domain name.

How developers can connect to the database using a bastion host:

In this scenario, you have a database hosted in a private subnet, and for security reasons, direct access to the database from the internet is restricted.
In this scenario, you have a database hosted in a private subnet, and for security reasons, direct access to the database from the internet is restricted.

- To connect to the database, developers can use a bastion host, which is an intermediate server that acts as a secure gateway. The bastion host is placed in the public subnet and is assigned a public IP address. Developers can establish an SSH connection to the bastion host using their SSH key pairs.

- Once connected to the bastion host, developers can then establish a secure connection to the database within the private subnet. They can use tools like SSH tunneling or port forwarding to forward the database port from the private subnet to the local machine through the bastion host. This allows them to securely interact with the database using their preferred database client or command-line tools.

- By using a bastion host, developers can maintain a secure and controlled access mechanism to the database, ensuring that only authorized individuals can connect to it while keeping the database isolated from direct internet exposure.

In summary, by utilizing an ALB, public users can access an EC2 instance in a private subnet through a domain name, while developers can securely connect to a database in the private subnet using a bastion host as an intermediary. These practices help maintain security and control while allowing necessary access to resources within private subnets.