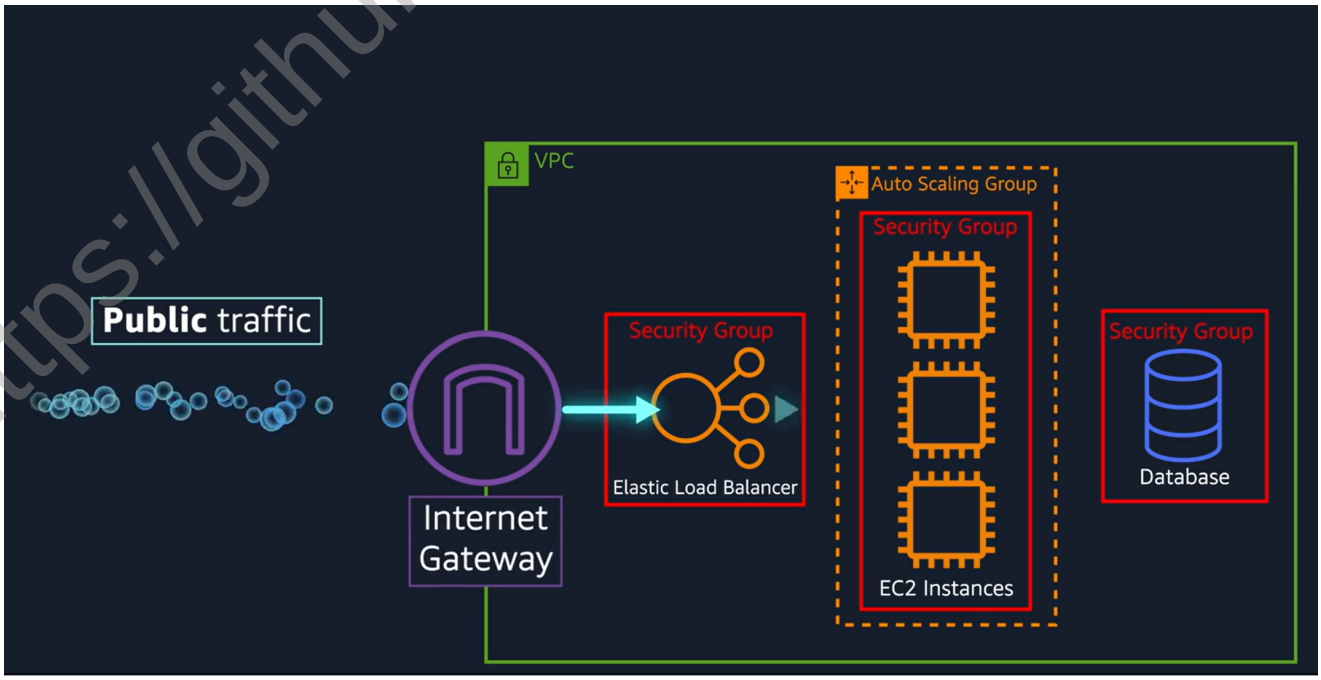
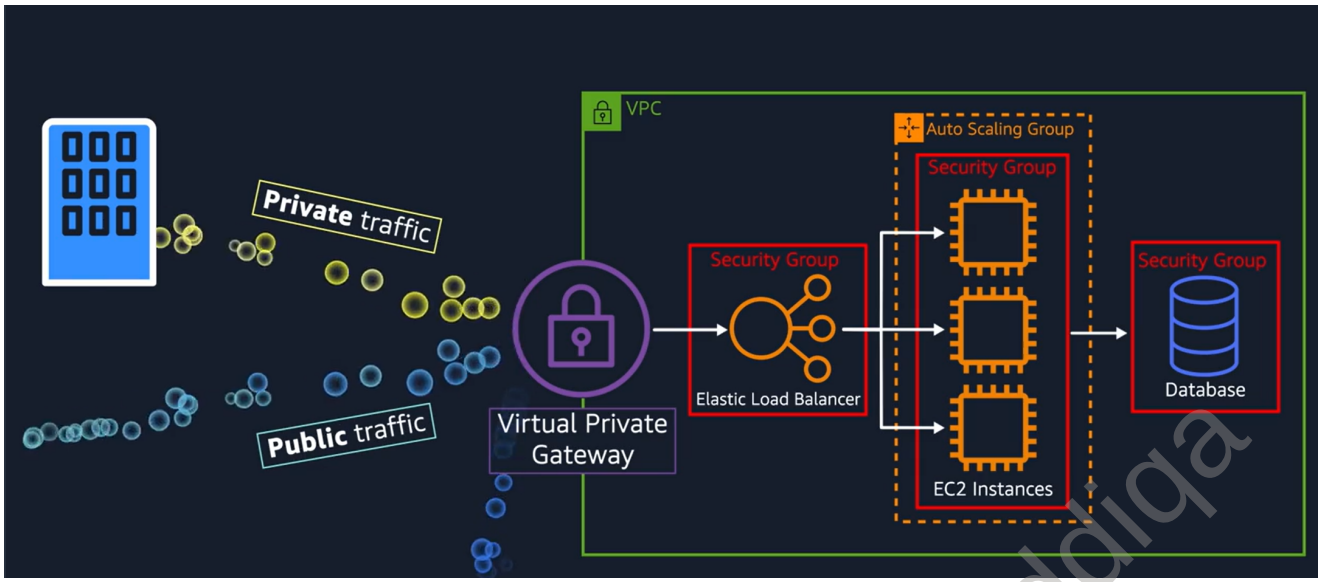
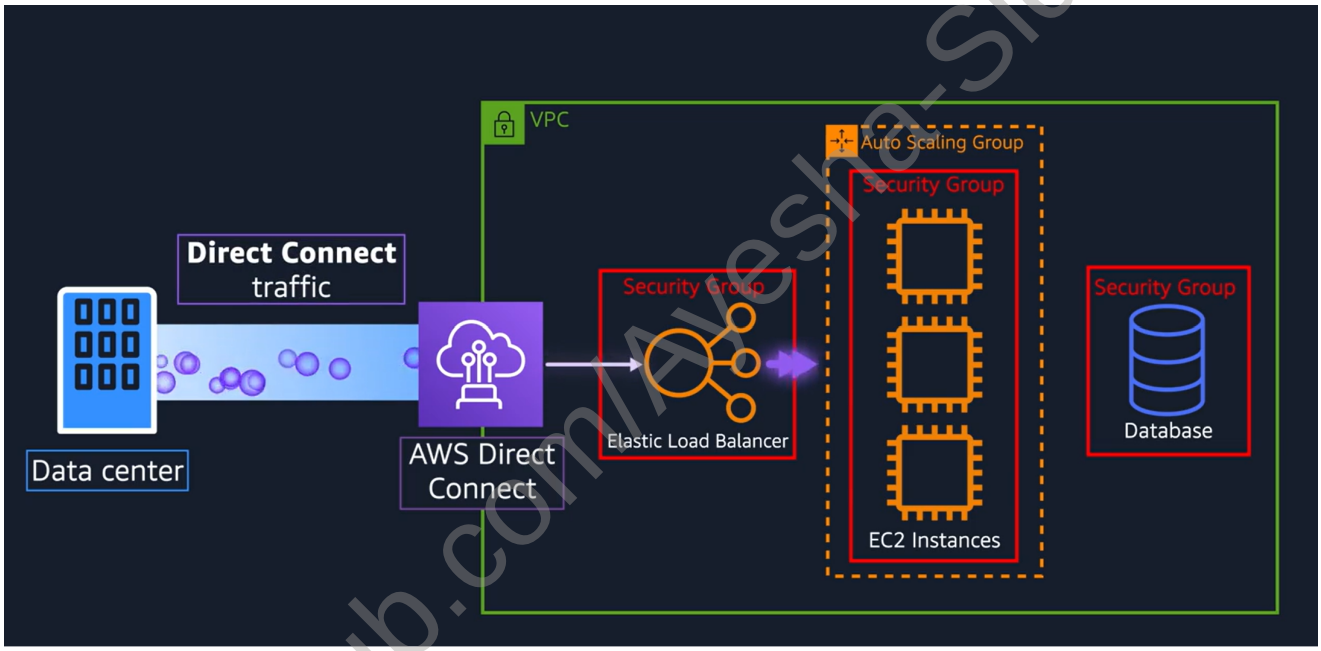
AWS Module 4 - Networking

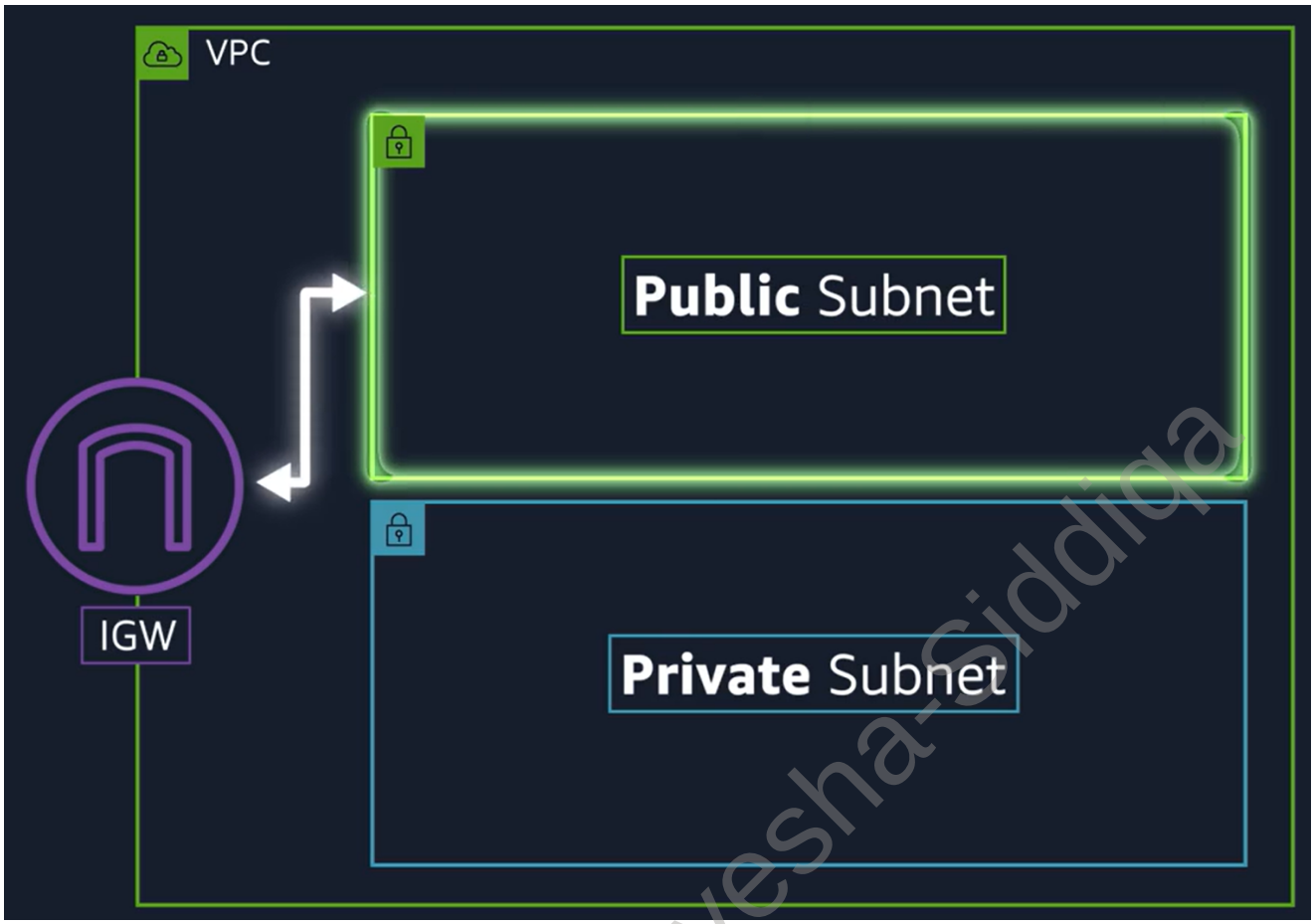
How does Amazon Virtual Private Cloud (Amazon VPC) provide boundaries for AWS resources, and what are the key networking services associated with it?

- **Amazon VPC:**
  - Establishes boundaries around AWS resources, allowing you to control network traffic.
  - Provides an isolated section of the AWS Cloud where you can launch resources within a defined virtual network.
  - Resources within a VPC can be organized into subnets, such as Amazon EC2 instances.
- **Internet Gateway:**
  - Acts as a connection between the VPC and the internet, similar to a doorway to a coffee shop.
  - Necessary for granting external access to resources in your VPC.
- **Virtual Private Gateway:**
  - Enables access to private resources within a VPC.
  - Works like a VPN connection, encrypting internet traffic for additional security.
  - Allows protected internet traffic to enter the VPC, but it shares the same road with other traffic.
- **AWS Direct Connect:**
  - Provides a dedicated private connection between your data center and a VPC.
  - Offers a high-bandwidth, low-latency connection that bypasses the public internet.
  - Analogous to a private hallway linking an apartment building to a coffee shop, reserved for specific users.









What is a subnet and what are the two types?

A subnet is a segment of a Virtual Private Cloud (VPC) in which resources are grouped based on security or operational requirements. There are two types of subnets within a VPC:

1. **Public Subnets:**
   - Public subnets contain resources that require accessibility by the public, such as websites for online stores.
   - These subnets host services that need to be reachable over the internet and are used for resources with public-facing functions.
2. **Private Subnets:**
   - Private subnets contain resources that should only be accessible through a private network, like databases housing sensitive customer information and order histories.
   - Resources in private subnets are isolated from direct external access, providing enhanced security.

What VPC component is responsible for checking packet permissions for subnets, and what is its role in managing network traffic within a VPC?

- **VPC Component for Packet Permissions:**
  - The VPC component responsible for checking packet permissions for subnets is a Network Access Control List (ACL).
- **Role of Network Access Control Lists (ACLs):**
  - ACLs are responsible for evaluating and enforcing packet permissions within subnets.

- They regulate the flow of network traffic in and out of subnets based on predefined rules and policies.

What is a Network Access Control List (ACL)?

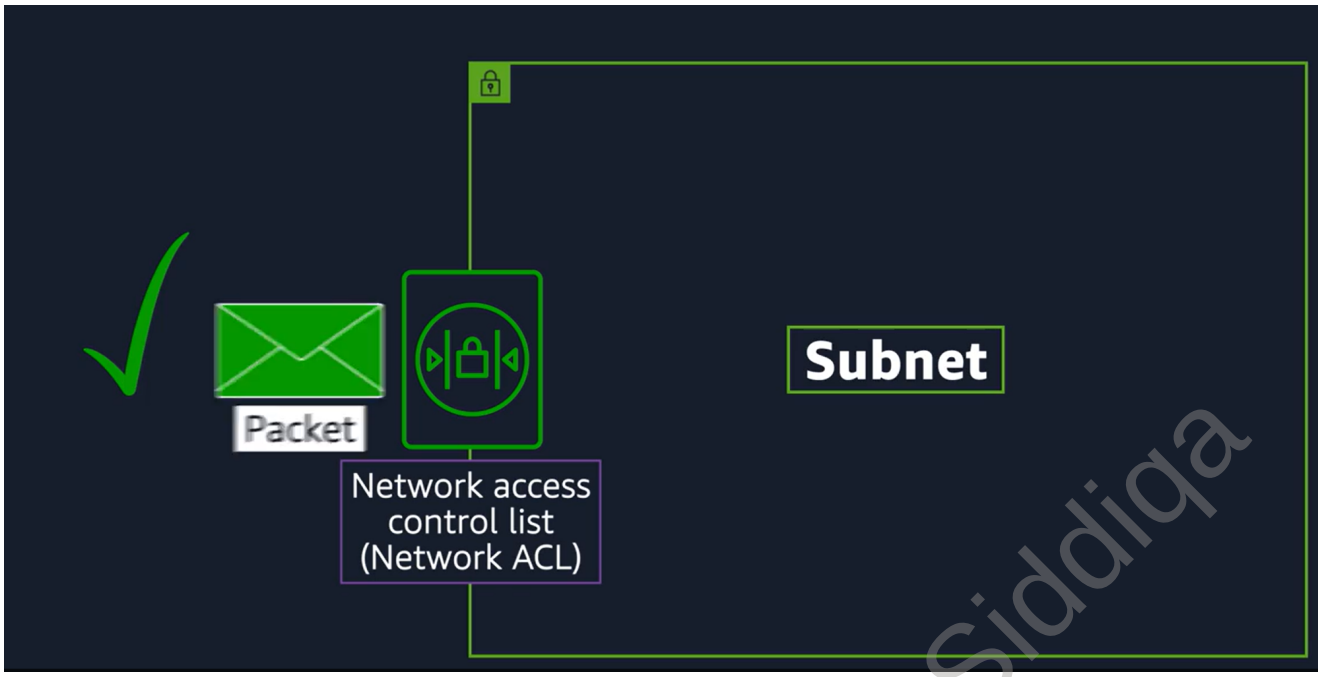
- A Network Access Control List (ACL) in AWS serves as a virtual firewall that controls both inbound and outbound network traffic at the subnet level.
- All network ACLs include an explicit deny rule to handle packets that don't match any other rules, preventing unauthorized access.
- Network Access Control Lists (ACLs) in AWS perform stateless packet filtering.
- Stateless filtering means that they don't maintain any memory or state information about network connections.
- By default, the account's default network ACL allows all inbound and outbound traffic but can be modified by adding specific rules.
- Custom network ACLs start with a default deny-all rule and require you to add rules for allowing specific traffic.

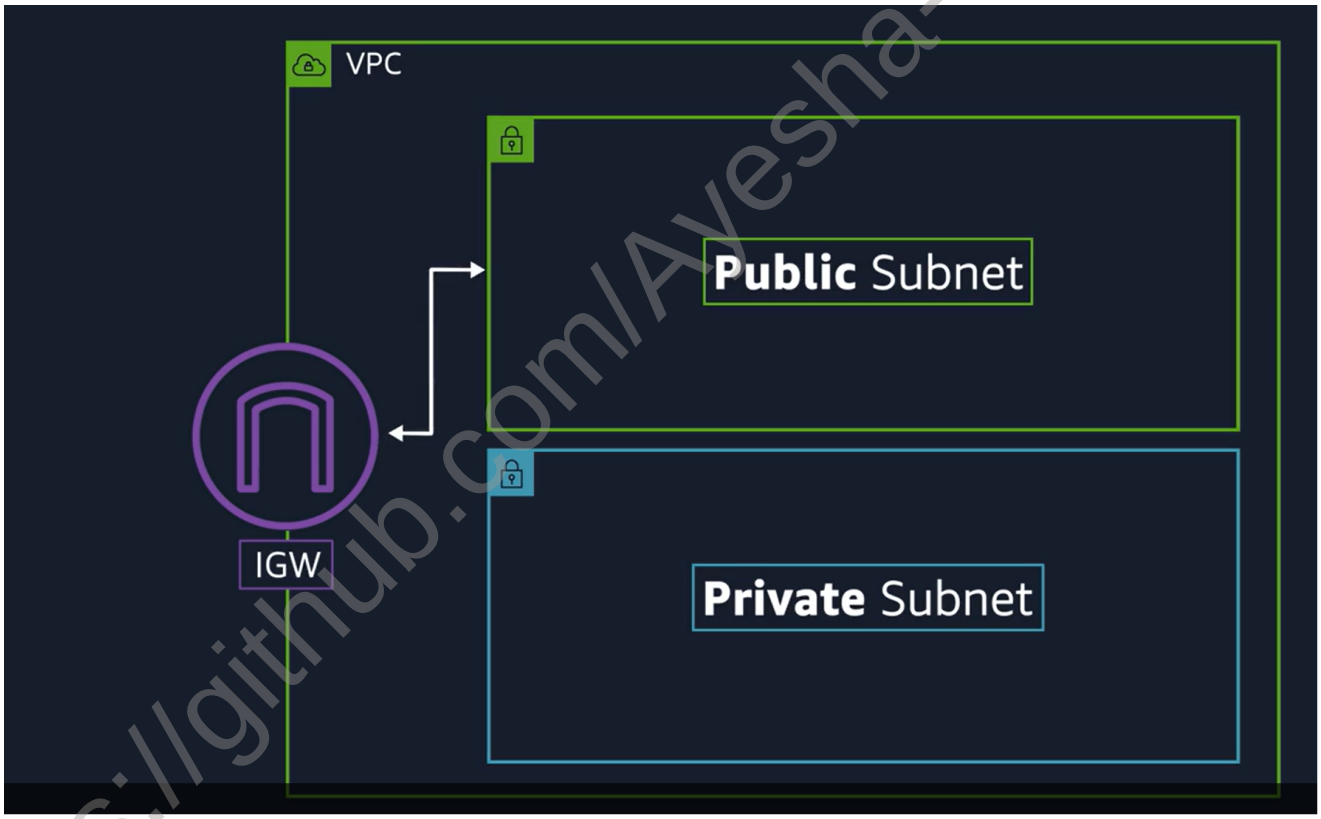
Which VPC component checks packet permissions for an Amazon EC2 instance?

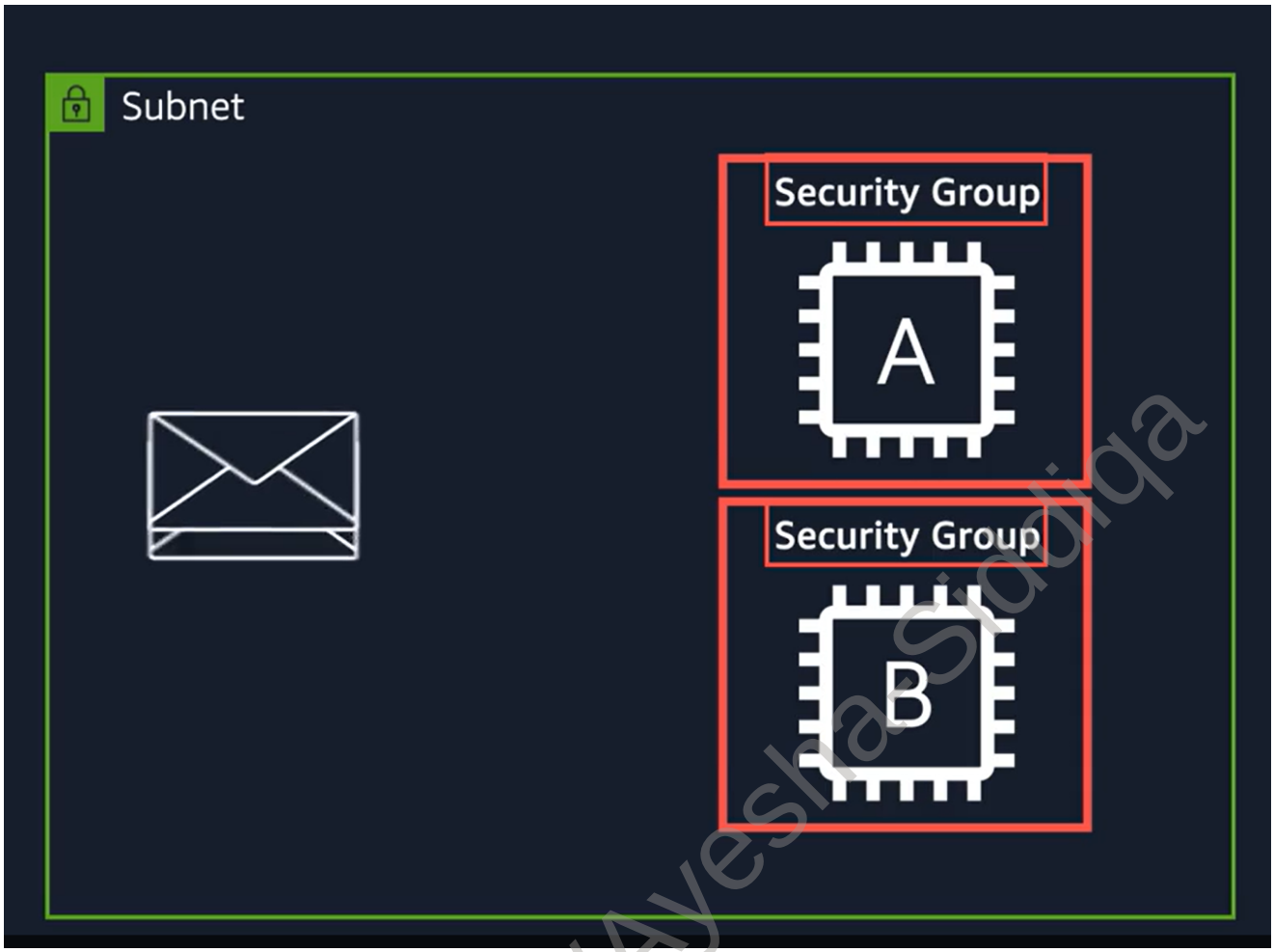
- A security group is a virtual firewall that controls inbound and outbound traffic for an Amazon EC2 instance.
- By default, a security group denies all inbound traffic and allows all outbound traffic.
- Security groups perform **stateful** packet filtering. They remember previous decisions made for incoming packets.

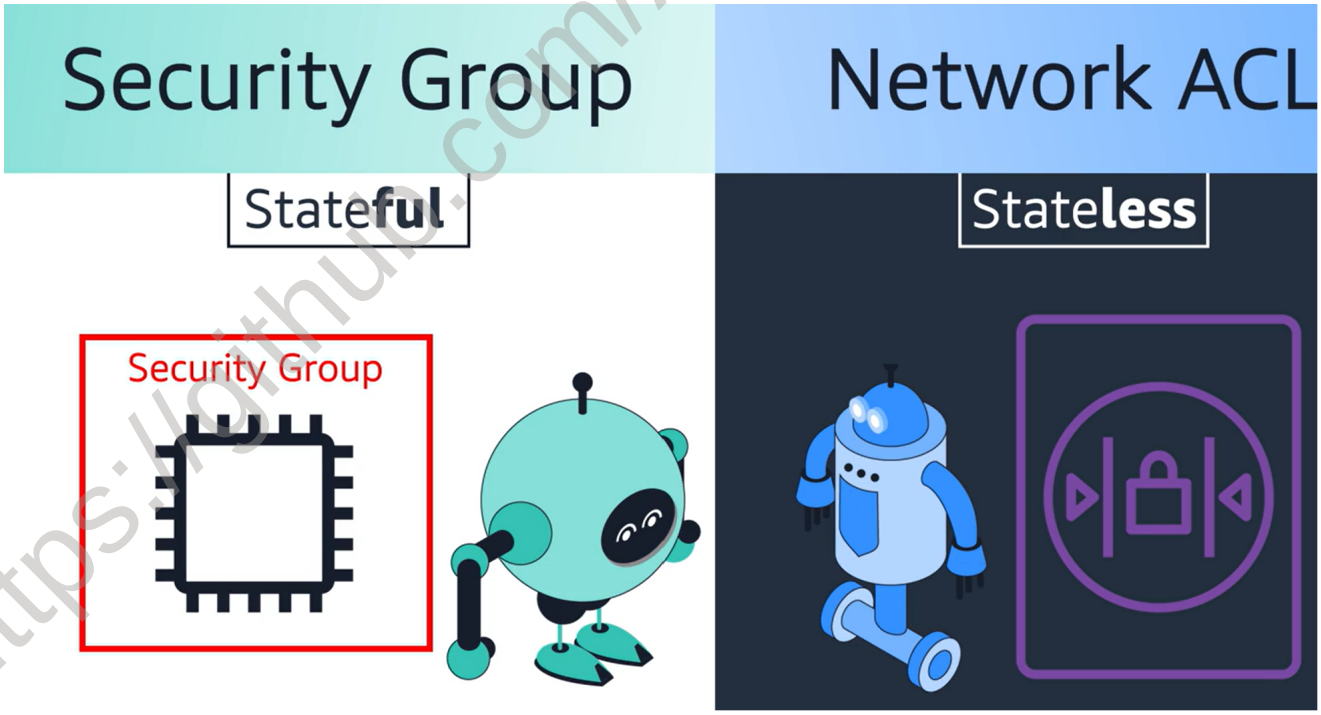
What is Amazon Route 53?

- Amazon Route 53 is a DNS web service provided by AWS.
- It offers a reliable way to direct end users to internet applications hosted within AWS infrastructure.
- Another key feature of Route 53 is its ability to manage DNS records for domain names.
- You can register new domain names directly within Route 53 and transfer DNS records for existing domains managed by other registrars.
- This centralized management of DNS records simplifies domain name management by allowing you to control all your domains from a single location.



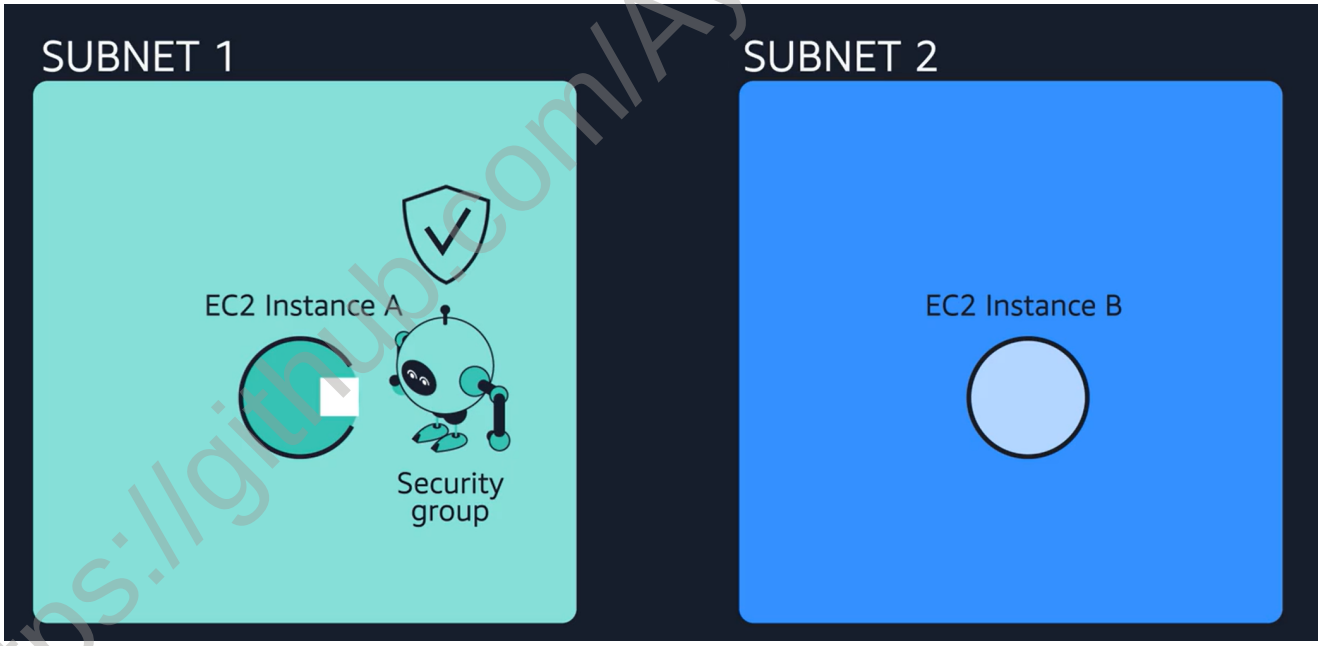


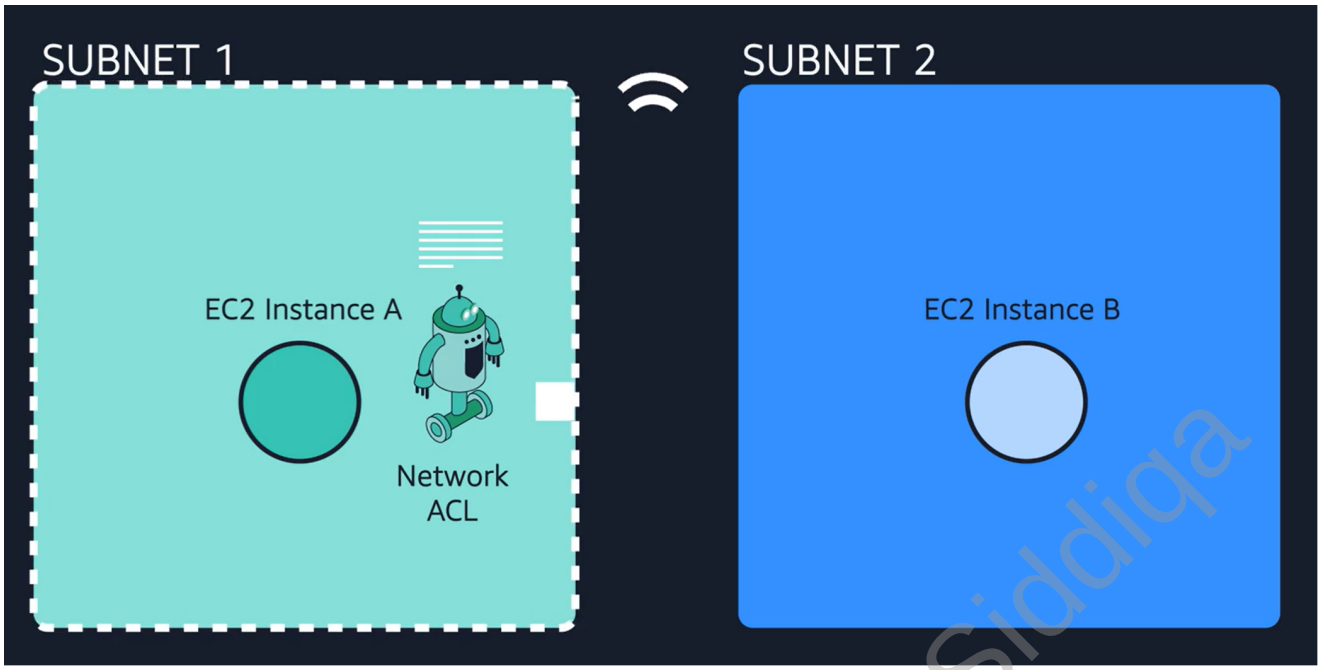


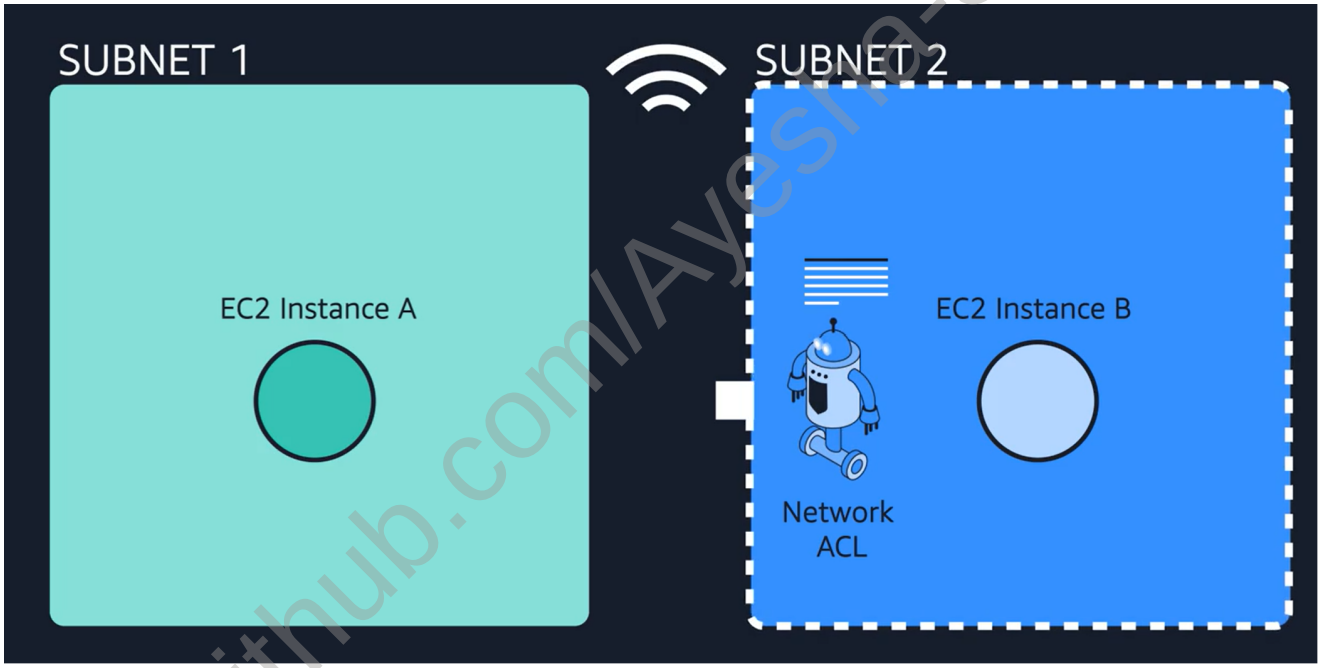


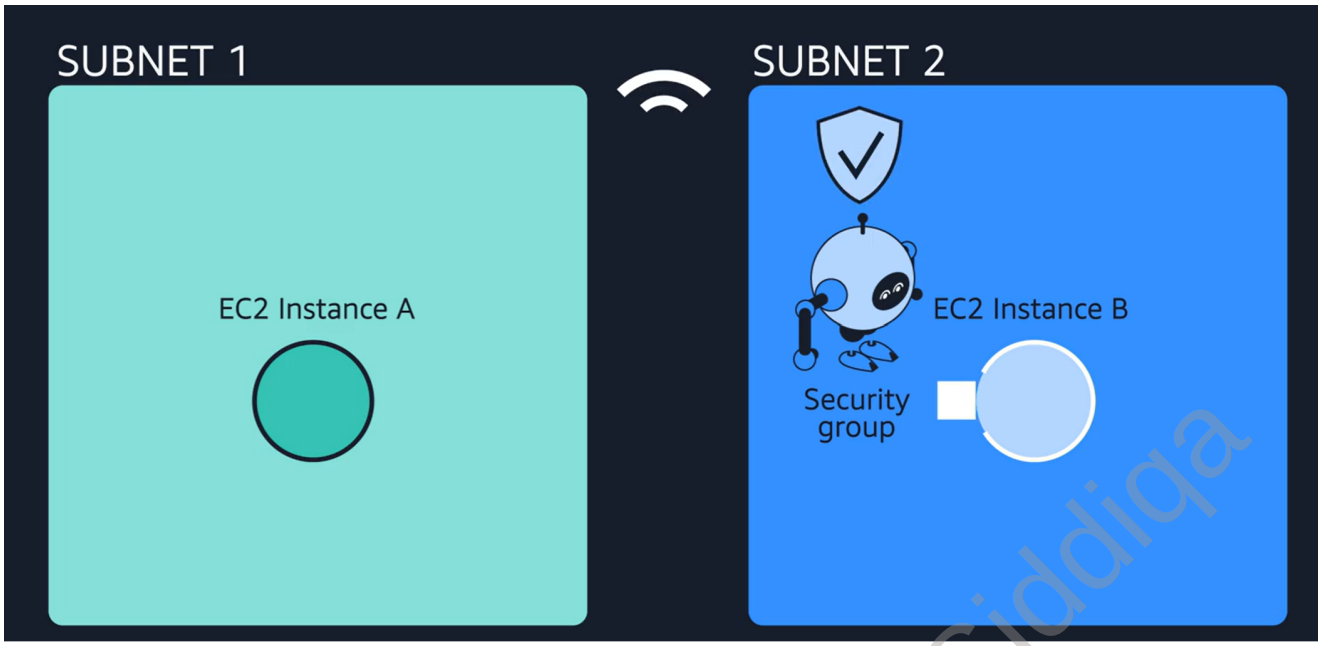
Which statement best describes an AWS account's default network access control list?

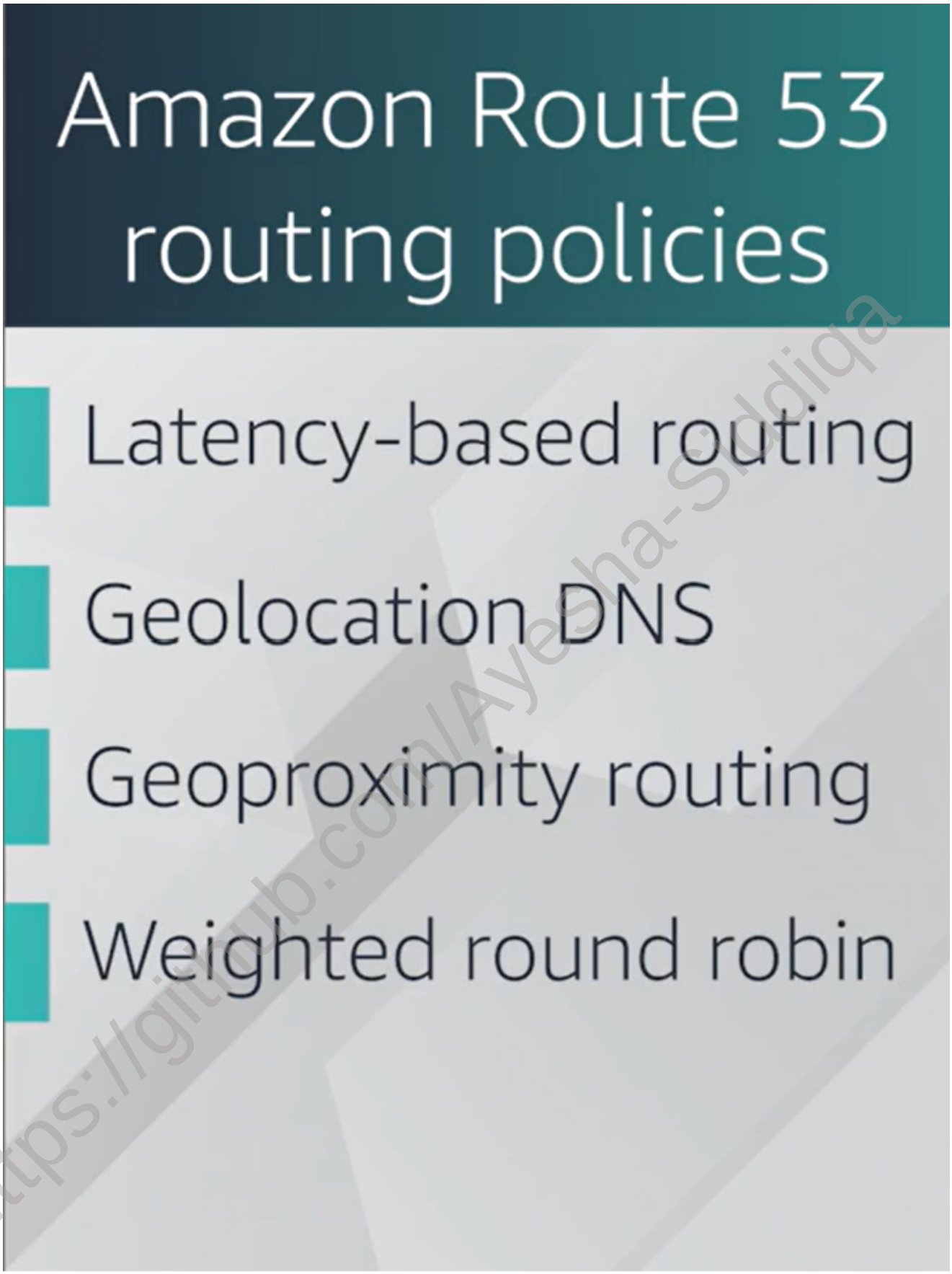
- ✗ It is stateless and denies all inbound and outbound traffic.
- ✗ It is stateful and allows all inbound and outbound traffic.
- ✓ It is stateless and allows all inbound and outbound traffic.
- ✗ It is stateful and denies all inbound and outbound traffic.











Content delivery network (CDN):
A network that delivers edge content to users based on their geographic location

Which statement best describes DNS resolution?

- ✗ Launching resources in a virtual network that you define
- ✗ Storing local copies of content at edge locations around the world
- ✗ Connecting a VPC to the internet
- ✓ Translating a domain name to an IP address

Your company has an application that uses Amazon EC2 instances to run the customer-facing website and Amazon RDS database instances to store customers' personal information. How should the developer configure the VPC according to best practices?

- ✗ Place the Amazon EC2 instances in a private subnet and the Amazon RDS database instances in a public subnet.
- ✓ Place the Amazon EC2 instances in a public subnet and the Amazon RDS database instances in a private subnet.
- ✗ Place the Amazon EC2 instances and the Amazon RDS database instances in a public subnet.
- ✗ Place the Amazon EC2 instances and the Amazon RDS database instances in a private subnet.

Which component can be used to establish a private dedicated connection between your company's data center and AWS?

- ✗ Private subnet
- ✗ DNS
- ✓ AWS Direct Connect
- ✗ Virtual private gateway

Correct

The correct response option is **AWS Direct Connect**.

The other response options are incorrect because:

- A private subnet is a section of a VPC in which you can group resources that should be accessed only through your private network. Although it is private, it is not used for establishing a connection between a data center and AWS.
- DNS stands for Domain Name System, which is a directory used for matching domain names to IP addresses.
- A virtual private gateway enables you to create a VPN connection between your VPC and a private network, such as your company's data center. Although this connection is private and encrypted, it travels through the public internet, not through a dedicated connection.

Which statement best describes security groups?

- [x] They are stateful and deny all inbound traffic by default.
- [ ] They are stateful and allow all inbound traffic by default.
- [ ] They are stateless and deny all inbound traffic by default.
- [ ] They are stateless and allow all inbound traffic by default.

Which component is used to connect a VPC to the internet?

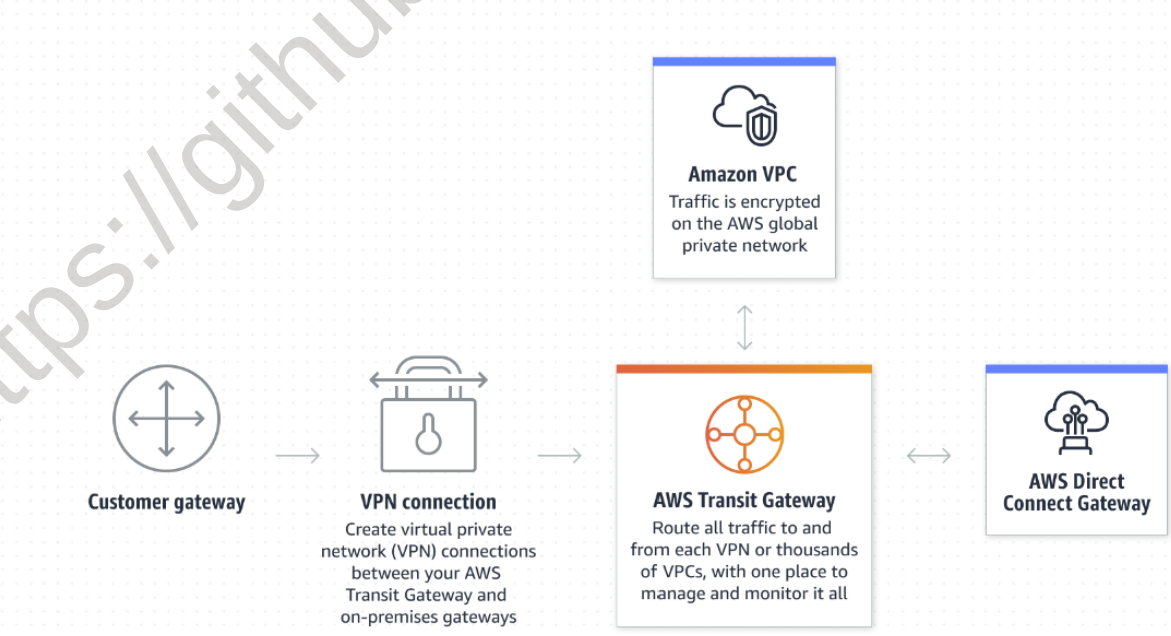
- [ ] Public subnet
- [ ] Edge location
- [ ] Security group
- [x] Internet gateway

Which service is used to manage the DNS records for domain names?

- ✗ Amazon Virtual Private Cloud
- ✗ AWS Direct Connect
- ✗ Amazon CloudFront
- ✓ Amazon Route 53

What is Transit gateway?

- AWS Transit Gateway connects your Amazon Virtual Private Clouds (VPCs) and on-premises networks through a central hub. This connection simplifies your network and puts an end to complex peering relationships. Transit Gateway acts as a highly scalable cloud router—each new connection is made only once.



What is AWS PrivateLink?

- AWS PrivateLink provides private connectivity between virtual private clouds (VPCs), supported AWS services, and your on-premises networks without exposing your traffic to the public internet. Interface VPC endpoints, powered by PrivateLink, connect you to services hosted by AWS Partners and supported solutions available in AWS Marketplace.

AWS networking and content delivery services

Network foundations

Amazon VPC
Customize and control your networking environment with Amazon Virtual Private Cloud (VPC)

AWS Transit Gateway
Simplify your network with VPCs and on-premises networks connected to a single gateway

AWS PrivateLink
Establish private connectivity between VPCs and AWS or on-premises services

Application networking

Amazon VPC Lattice
Simplify service-to-service connectivity, security, and monitoring

AWS AppMesh
Connect containers and microservices with application-level networking

AWS API Gateway
Create, maintain, and secure APIs at any scale

AWS Cloud Map
Discover and access the most up-to-date service resources

Elastic Load Balancing
Distribute network traffic to improve application scalability

Edge networking

Amazon CloudFront
Deliver data, videos, applications, and APIs at high transfer speeds with low latency

Amazon Route 53
Drive end users to internet applications with a low-cost managed Domain Name System (DNS)

AWS Global Accelerator
Optimize user traffic to your application

Hybrid connectivity

AWS Direct Connect
Establish a private, dedicated AWS connection to your data center, office, or colocation environment

AWS Site-to-Site VPN
Create an encrypted network connection to your Amazon VPCs or AWS Transit Gateways

AWS Client VPN
Connect your remote workforce to AWS or on-premises with a Virtual Private Network (VPN)

AWS Cloud WAN
Easily build, manage, and monitor global wide area networks

Network security

AWS Shield
Safeguard AWS applications against distributed denial of service (DDoS) attacks

AWS WAF
Protect your web applications from common web exploits

AWS Network Firewall
Deploy network security across your Amazon VPCs

AWS Firewall Manager
Centrally configure and manage firewall rules