Agenda

- **Network ACLs (Network Access Control List)**
- **VPC Endpoints**
- **VPC peering**


what
have you
Learned

Q-1. Which statement describes Amazon Virtual Private Cloud (Amazon VPC) ?

- It is a highly available and scalable Domain Name System (DNS) web services.
- It is used to manage only public networks in the AWS Cloud
- It enables you to create a private network in the AWS Cloud
- It is an on-premises network

Q-1. Which statement describes Amazon Virtual Private Cloud (Amazon VPC) ?

- It is a highly available and scalable Domain Name System (DNS) web services.
- It is used to manage only public networks in the AWS Cloud
- It enables you to create a private network in the AWS Cloud (correct)
- It is an on-premises network

Q-2. Which resource must be specified when creating a virtual private cloud(VPC) ?

- Amazon Elastic Compute Cloud (Amazon EC2) instance
- Elastic Load Balancing load balancer
- IP address range
- Linux system

Q-2. Which resource must be specified when creating a virtual private cloud(VPC) ?

- Amazon Elastic Compute Cloud (Amazon EC2) instance
- Elastic Load Balancing load balancer
- IP address range (correct)
- Linux system

Q-3. Which resource would benefit from being in a private subnet?

- A database
- An Amazon Elastic Compute Cloud (Amazon EC2) instance hosting a website with a public IP address that must be accessed from the internet
- A company site that requires both external access and internal access from the public and its employees
- A public website

Q-3. Which resource would benefit from being in a private subnet?

- A database (Correct)
- An Amazon Elastic Compute Cloud (Amazon EC2) instance hosting a website with a public IP address that must be accessed from the internet
- A company site that requires both external access and internal access from the public and its employees
- A public website

Q-4. What is the purpose of a route table?

- It limits traffic by allowing only specified IP addresses.
- It determines where all traffic is directed outside the virtual private cloud (VPC).
- It is responsible for only the network traffic in a subnet.
- It determines where network traffic is directed within the virtual private cloud (VPC)

Q-4. What is the purpose of a route table?

- It limits traffic by allowing only specified IP addresses.
- It determines where all traffic is directed outside the virtual private cloud (VPC).
- It is responsible for only the network traffic in a subnet.
- It determines where network traffic is directed within the virtual private cloud (VPC) (correct)

Q-5. Which statement describes a security group?

- It acts as a stateless firewall that controls inbound traffic only.
- It acts as a stateless firewall that controls outbound network traffic only.
- It acts as a stateful firewall that controls inbound network traffic and outbound network traffic.
- It acts as a stateful firewall that allows all traffic by default.

Q-5. Which statement describes a security group?

- It acts as a stateless firewall that controls inbound traffic only.
- It acts as a stateless firewall that controls outbound network traffic only.
- It acts as a stateful firewall that controls inbound network traffic and outbound network traffic. (Correct)
- It acts as a stateful firewall that allows all traffic by default.

Q-6. What are some reasons for creating a subnet ?

- To reduce network traffic
- To reduce the number of networks to manage
- To divide a network into smaller, more efficient subnets
- To add additional IP addresses to an existing subnet
- To allocate a specific static IP address

Q-6. What are some reasons for creating a subnet ?

- To reduce network traffic (correct)
- To reduce the number of networks to manage
- To divide a network into smaller, more efficient subnets (correct)
- To add additional IP addresses to an existing subnet
- To allocate a specific static IP address

Q-7. An administrator creates a subnet with a classes inter-domain routing (CIDR) range of 10.0.0./24 how many IP addresses can the administrator assign to hosts in this subnets?

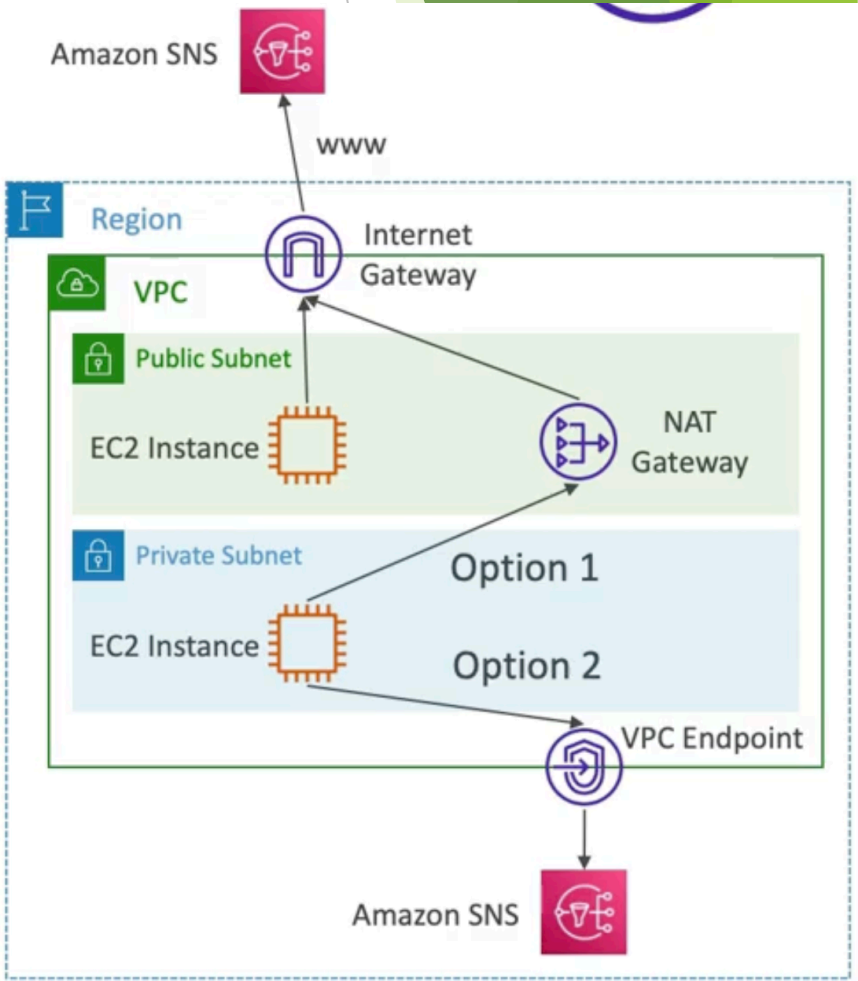
- 256
- 1024
- 24
- 512

VPC endpoints

“What can we do to keep our connections to AWS services private?”

VPC Endpoints (AWS Private-Link)

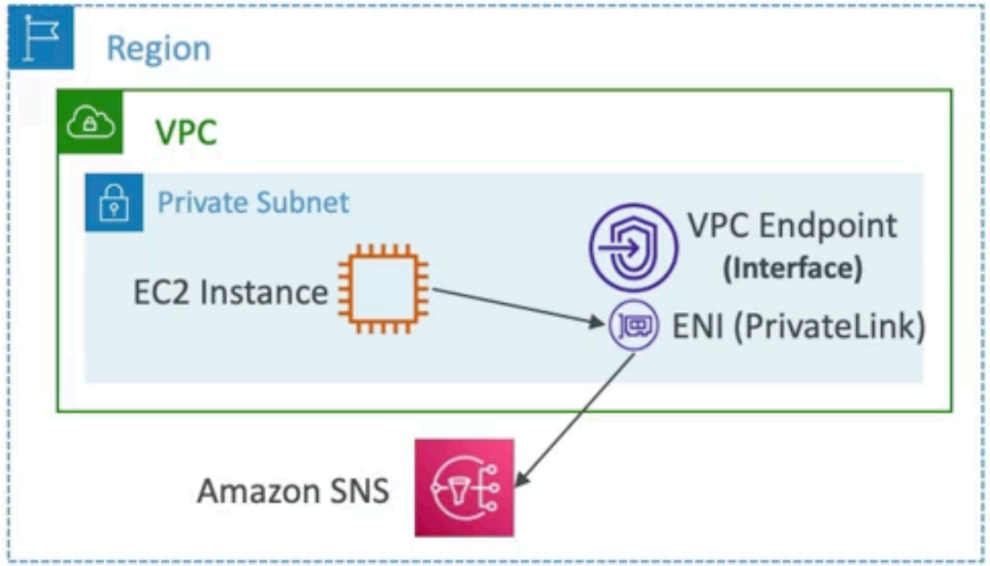
- Every AWS service is publicly exposed (public URL)
- VPC Endpoint (powered by AWS Private-Link) allows you to connect to AWS services using a private network instead of using the public Internet
- They're redundant and scale horizontally
- They remove the need of IGW, NATGW… to access AWS services
- In Case of issues:
  - Check DNS setting Resolution in your VPC
  - Check Route Tables

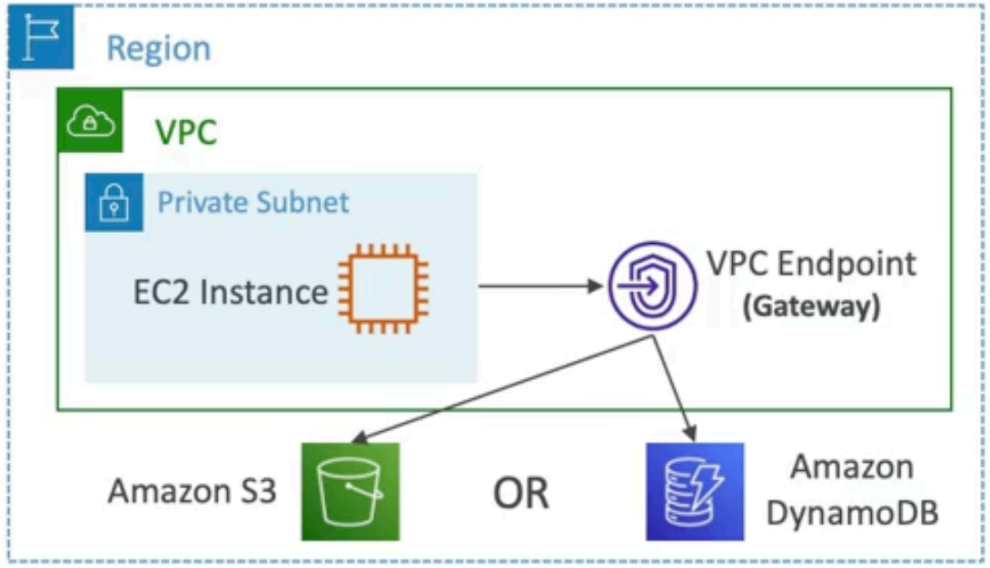


Types of Endpoints

- Interface Endpoints (powered by Private Link)
  - Provisions and ENI (private IP address) as an entry point (Must attach a Security Group)
  - Supports most AWS services
  - $ per hour + $ per GB of data processed

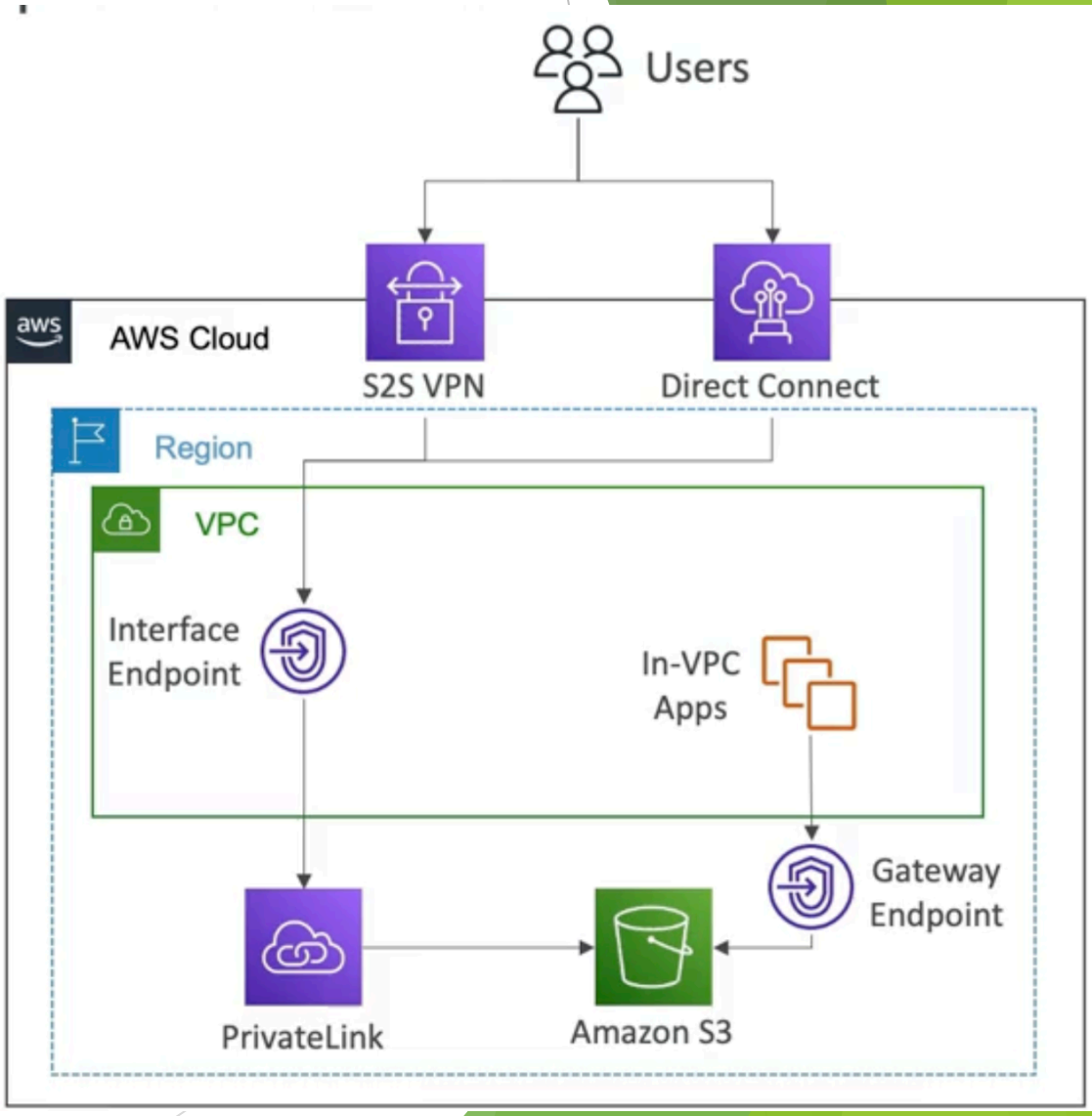
- Gateway Endpoints
  - Provisions a gateway and must be used as a target in a route table (does not use security groups)
  - Supports both S3 and DynamoDB
  - free





Gateway or Interface Endpoint for S3

- Gateway is most likely going to be preferred all the time at the exam
- Cost : free for gateway, $ for interface endpoint
- Interface Endpoint is preferred access is required from on-premises (site to site VPN or Direct Connect), a different VPC or a different region



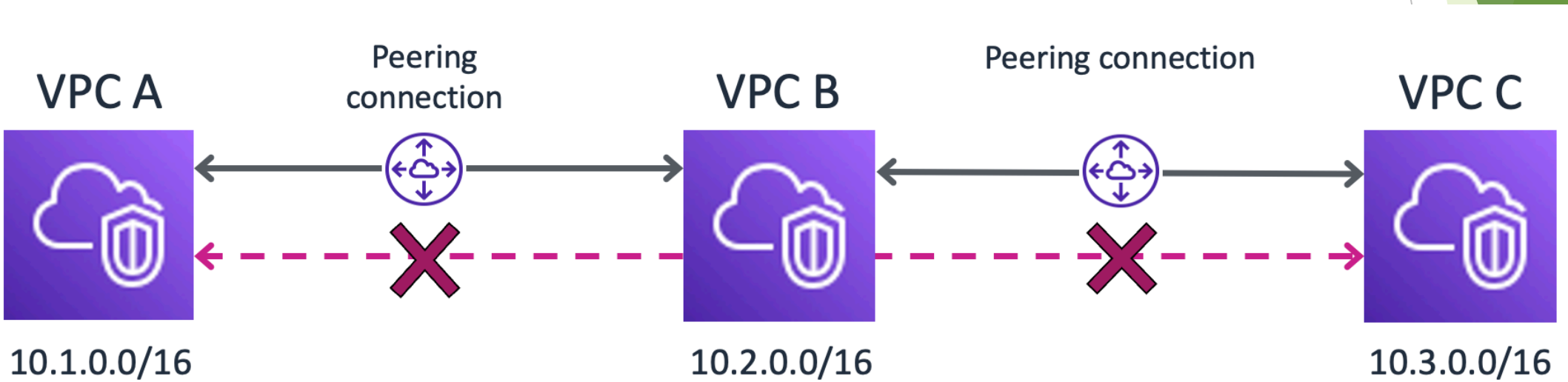
Useful commands

- #curl google.com
- #aws s3 ls –region ap-south-1
- #curl 10.0.0.72:80/ (showing web page content)

VPC Peering

“How can we privately route traffic between our VPCs”

Multiple VPC peering conections



Note: No transitive peering relationships

VPC Peering

- Privately connect two VPCs using AWS network
- Make them behaves as if they were in the same network
- Must not have overlapping CIDRs
- VPC Peering connection in NOT transitive (must be established for each VPC that need to communicate with one another)
- You must update route tables in each VPC's subnets to ensure EC2 instances can communicate with each other