

VPC Overview

1. So VPC stands for virtual private cloud and this is going

VPC – Crash Course

- VPC is something you should know in depth for the AWS Certified Solutions Architect Associate & AWS Certified SysOps Administrator
- At the AWS Certified Cloud Practitioner Level, you should know about:
 - VPC, Subnets, Internet Gateways & NAT Gateways
 - Security Groups, Network ACL (NACL), VPC Flow Logs
 - VPC Peering, VPC Endpoints
 - Site to Site VPN & Direct Connect
 - Transit Gateway
- I will just give you an overview, less than 1 or 2 questions at your exam.
- We'll have a look at the "default VPC" (created by default by AWS for you)
- There is a summary lecture at the end. It's okay if you don't understand it all

2.

IP Addresses in AWS

IP Addresses in AWS

- IPv4 – Internet Protocol version 4 (4.3 Billion Addresses)
 - Public IPv4 – can be used on the Internet
 - EC2 instance gets a new a public IP address every time you stop then start it (default)
 - Private IPv4 – can be used on private networks (LAN) such as internal AWS networking (e.g., 192.168.1.1)
- 1.
 - Private IPv4 is fixed for EC2 Instances even if you start/stop them
 - Elastic IP – allows you to attach a fixed public IPv4 address to EC2 instance
- • Note: has ongoing cost if not attached to EC2 instance or if the EC2 instance is stopped
- IPv6 – Internet Protocol version 6 (3.4×10^{38} Addresses)
 - Every IP address is public (no private range)
 - Example: 2001:db8:3333:4444:cccc:dddd:eeee:ffff

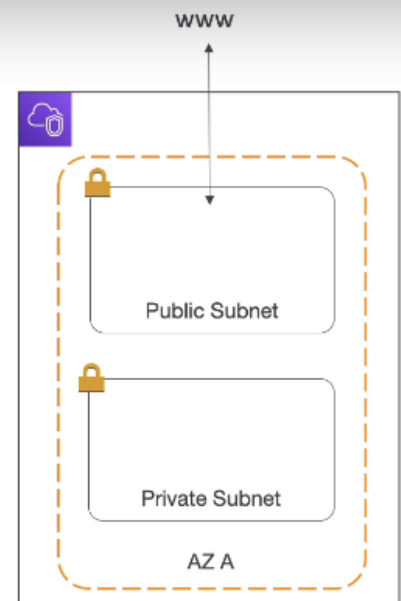
2.


VPC & Subnets Primer

1. VPC is a private cloud..here we can store our ec2 instances etc..
2. Vpc is linked to specific region...if we have multiple regions in AWS..we can have multiple vpc

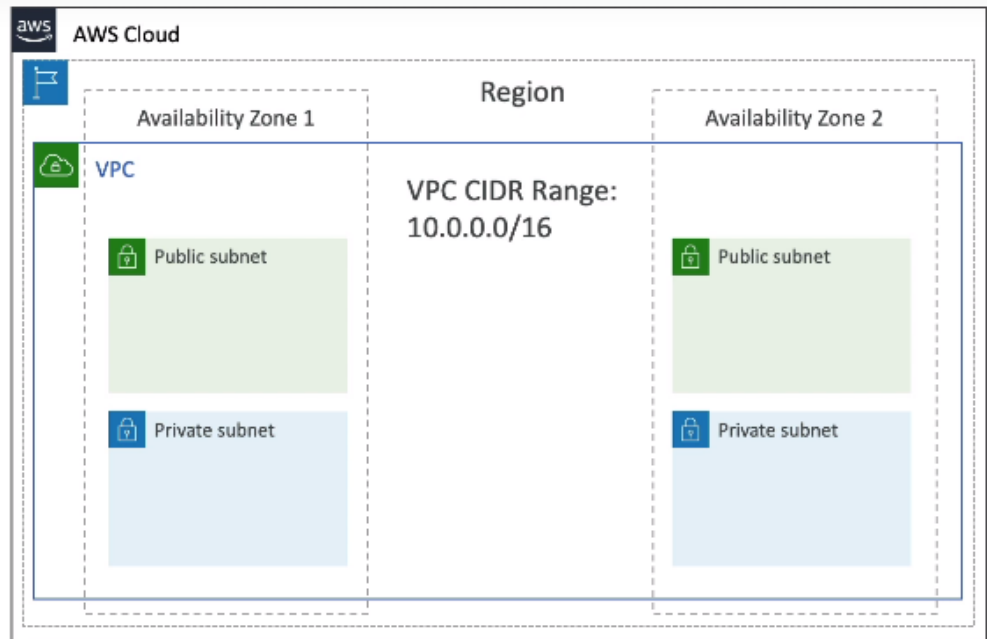
VPC & Subnets Primer

- VPC - Virtual Private Cloud: private network to deploy your resources (regional resource)
- Subnets allow you to partition your network inside your VPC (Availability Zone resource)
- A public subnet is a subnet that is accessible from the internet
- A private subnet is a subnet that is not accessible from the internet
- To define access to the internet and between subnets, we use Route Tables.



3. 
4. Here in the AZ..we have public and private subnet
5. Here in public subnet we can store our ec2 instance and in private subnet we can store db's ..as db's need more security
6. VPC diagram

VPC Diagram



- 7.
8. Here in the diagram..in one region we have one vpc..in the region we have 2AZ's and they subnets in them

VPC CIDR range in AWS VPC stands for Virtual Private Cloud Classless Inter-Domain Routing range. It is a range of IP addresses that are used to identify and route traffic within a VPC. The CIDR range must be unique within a region and cannot overlap with any other VPC CIDR range.

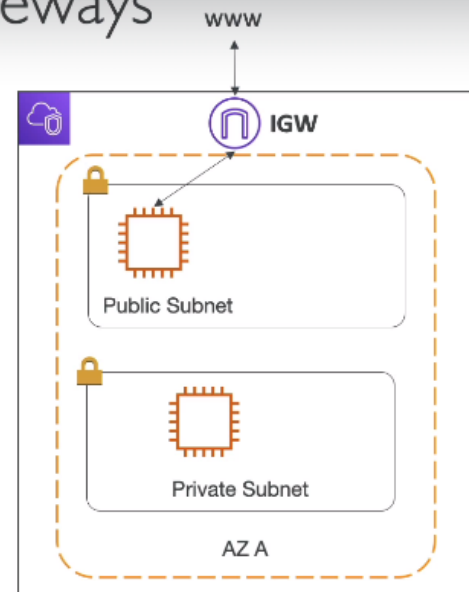
The default CIDR range for a VPC is 10.0.0.0/16. This means that the first 16 bits of the IP address are used to identify the VPC and the remaining 16 bits are used to identify the host within the VPC.

You can change the CIDR range for a VPC at any time. However, you must ensure that the new CIDR range does not overlap with any other VPC CIDR range.

- 9.
10. Internet Gateway & NAT Gateways

Internet Gateway & NAT Gateways

- Internet Gateways helps our VPC instances connect with the internet
- Public Subnets have a route to the internet gateway.
- NAT Gateways (AWS-managed) & NAT Instances (self-managed) allow your instances in your Private Subnets to access the internet while remaining private



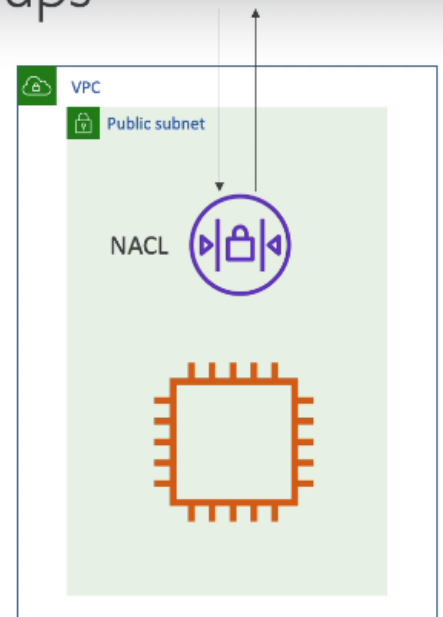
11. _____
12. Here we have an instance in public subnet..for that instance to access the internet it needs a internet Gateway which routes to the internet
13. NAT gateways are used fot private subnets to access internet

NACL and Security Groups

1. NACL are firewall at subnet level...
2. Lets suppose we have an ec2 instance ..And the first line of defense for our EC2 Instance, is a NACL or a Network ACL, which is a firewall that is controlling traffic from and to the subnets.

Network ACL & Security Groups

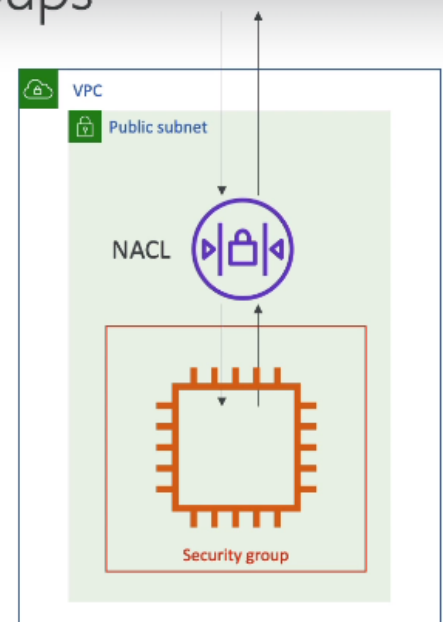
- NACL (Network ACL)
 - A firewall which controls traffic from and to subnet
 - Can have ALLOW and DENY rules
 - Are attached at the Subnet level
 - Rules only include IP addresses



3.

Network ACL & Security Groups

- NACL (Network ACL)
 - A firewall which controls traffic from and to subnet
 - Can have ALLOW and DENY rules
 - Are attached at the Subnet level
 - Rules only include IP addresses
- Security Groups
 - A firewall that controls traffic to and from an ENI / an EC2 Instance
 - Can have only ALLOW rules
 - Rules include IP addresses and other security groups



4.

5. So NACL is at subnet level and security grps are at ec2 instance level

Network ACLs vs Security Groups

Security Group	Network ACL
Operates at the instance level	Operates at the subnet level
Supports allow rules only	Supports allow rules and deny rules
Is stateful: Return traffic is automatically allowed, regardless of any rules	Is stateless: Return traffic must be explicitly allowed by rules
We evaluate all rules before deciding whether to allow traffic	We process rules in number order when deciding whether to allow traffic
Applies to an instance only if someone specifies the security group when launching the instance, or associates the security group with the instance later on	Automatically applies to all instances in the subnets it's associated with (therefore, you don't have to rely on users to specify the security group)

6.

VPC Flow Logs

VPC Flow Logs



- Capture information about IP traffic going into your interfaces:
 - VPC Flow Logs
 - Subnet Flow Logs
 - Elastic Network Interface Flow Logs
- Helps to monitor & troubleshoot connectivity issues. Example:
 - Subnets to internet
 - Subnets to subnets
 - Internet to subnets
- Captures network information from AWS managed interfaces too: Elastic Load Balancers, ElastiCache, RDS, Aurora, etc...
- VPC Flow logs data can go to S3, CloudWatch Logs, and Kinesis Data Firehose

1.

VPC flow logs in AWS VPC are a record of network traffic that flows into and out of your VPC. They can be used to monitor network traffic, troubleshoot network issues, and collect data for security analysis.

Here are some of the things you can do with VPC flow logs:

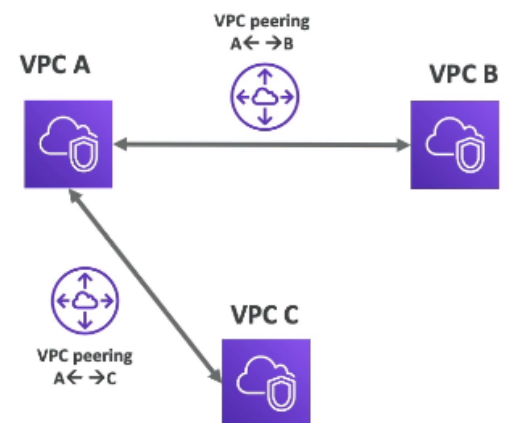
- **Monitor network traffic:** You can use VPC flow logs to see what traffic is flowing into and out of your VPC. This can help you to identify potential security threats or performance bottlenecks.
- **Troubleshoot network issues:** If you are experiencing network issues, you can use VPC flow logs to troubleshoot the issue. You can see where the traffic is coming from and going to, and you can identify any dropped packets.
- **Collect data for security analysis:** You can use VPC flow logs to collect data for security analysis. This data can be used to identify potential threats, such as unauthorized access or denial-of-service attacks.

2.

VPC Peering

- Connect two VPC, privately using AWS' network
- Make them behave as if they were in the same network
- Must not have overlapping CIDR (IP address range)
- VPC Peering connection is **not transitive** (must be established for each VPC that need to communicate with one another)

3.



Sure. Let's say you have two VPCs:

- VPC A: This VPC contains your web servers.
- VPC B: This VPC contains your database servers.

You want to be able to route traffic between your web servers and your database servers without having to use an internet gateway or VPN.

You can do this by creating a VPC peering connection between VPC A and VPC B.

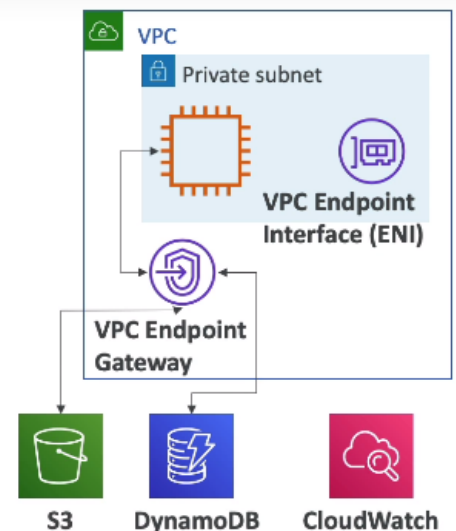
Once you have created the VPC peering connection, you can route traffic between your web servers and your database servers using the VPC peering connection.

4.

VPC Endpoints - interface & gateway

VPC Endpoints

- Endpoints allow you to connect to AWS Services using a private network instead of the public www network
- This gives you enhanced security and lower latency to access AWS services
- VPC Endpoint Gateway: S3 & DynamoDB
- VPC Endpoint Interface: the rest

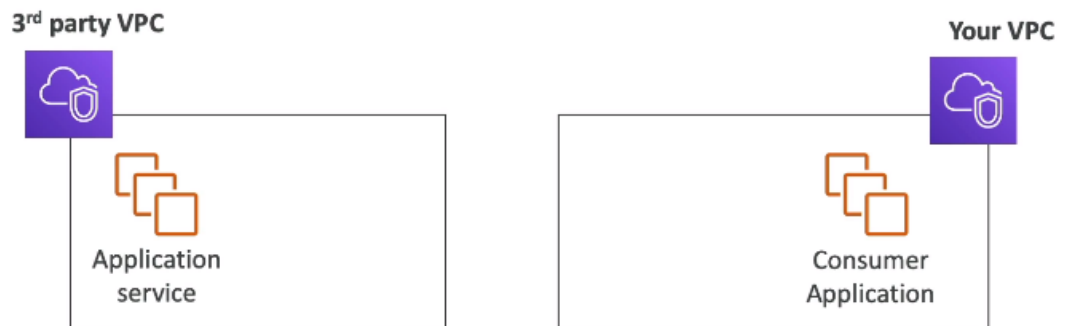


1.

AWS Private Links

AWS PrivateLink (VPC Endpoint Services)

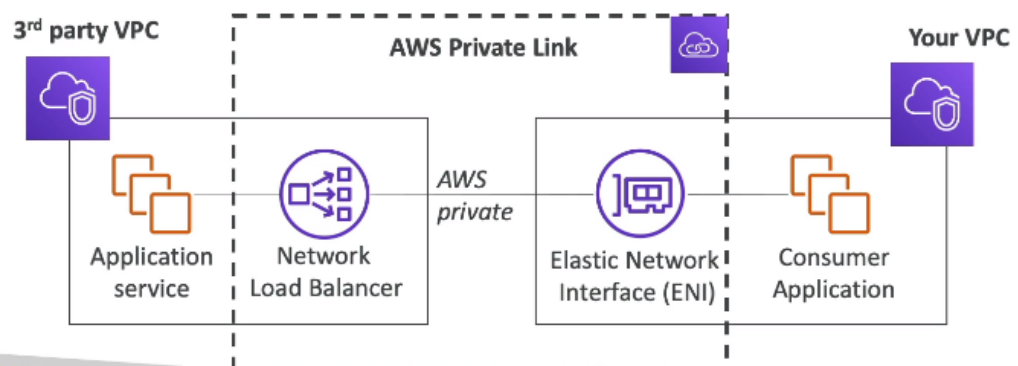
- Most secure & scalable way to expose a service to 1000s of VPCs
- Does not require VPC peering, internet gateway, NAT, route tables...
- Requires a network load balancer (Service VPC) and ENI (Customer VPC)



1.

AWS PrivateLink (VPC Endpoint Services)

- Most secure & scalable way to expose a service to 1000s of VPCs
- Does not require VPC peering, internet gateway, NAT, route tables...
- Requires a network load balancer (Service VPC) and ENI (Customer VPC)



2.

What is AWS PrivateLink used for?

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.

3.

Preventing sensitive data from travelling over the Internet, such as customer records, helps users stay in compliance with rules like HIPAA, EU/US Privacy Shield, and PCI. Customers in the financial services, healthcare, and government sectors will benefit the most from this. AWS PrivateLink keeps

4.

Direct Connect and Site 2 Site

1. Lets say we have our onpremises data center and if we need to connect to the cloud to our vpc
2. We have 2 options one is site to site vpn

Site to Site VPN & Direct Connect

• Site to Site VPN

- Connect an on-premises VPN to AWS
- The connection is automatically encrypted
- Goes over the public internet



3.

4. In about five minutes,

5. you can have a connection between your data center in AWS.

6. But it goes over the public internet, so you may have some limited bandwidth and you may have some security concerns, even though it is obviously encrypted.

7. The other option is to use Direct connect or DX

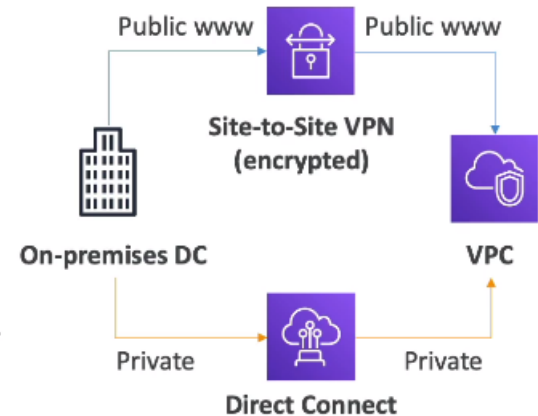
Site to Site VPN & Direct Connect

- Site to Site VPN

- Connect an on-premises VPN to AWS
- The connection is automatically encrypted
- Goes over the public internet

- Direct Connect (DX)

- Establish a physical connection between on-premises and AWS
- The connection is private, secure and fast
- Goes over a private network
- Takes at least a month to establish



8.

9. In site to site...lets suppose we have our ec2 instance in private subnet in a vpc

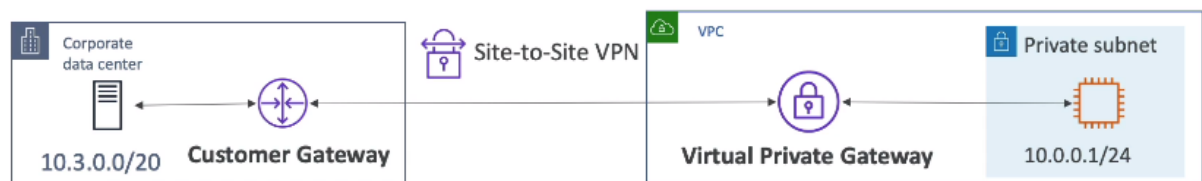
10. So for this, to establish a site-to-site VPN,

11. we need on-premises a customer gateway or CGW,

12. and that's something you have to remember at the exam. So it's a customer gateway, or CGW and then on the AWS site you will need virtual private gateway, or VGW and once the two things are provisioned and created, then you can connect them together using a site-to-site VPN.

Site-to-Site VPN

- On-premises: must use a Customer Gateway (CGW)
- AWS: must use a Virtual Private Gateway (VGW)

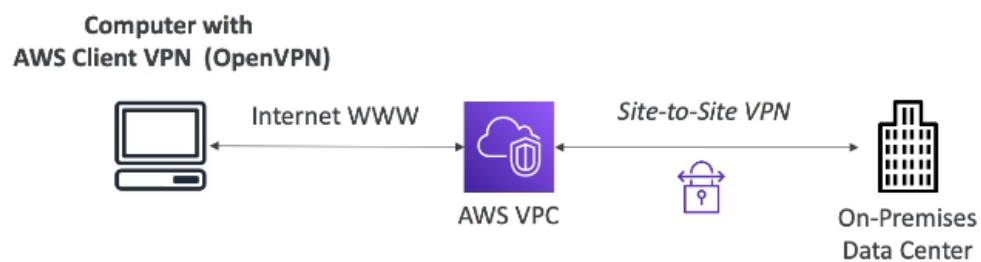


13.

AWS Client VPN



- Connect from your computer using OpenVPN to your private network in AWS and on-premises
- Allow you to connect to your EC2 instances over a private IP (just as if you were in the private VPC network)
- Goes over public Internet



1.

Sure. AWS Client VPN is a service that allows you to securely connect to your AWS resources from your computer or mobile device, even when you are not on your corporate network.

AWS Client VPN uses IPsec to encrypt all traffic between your device and your AWS resources. This ensures that your traffic is secure even if you are connecting to a public Wi-Fi network.

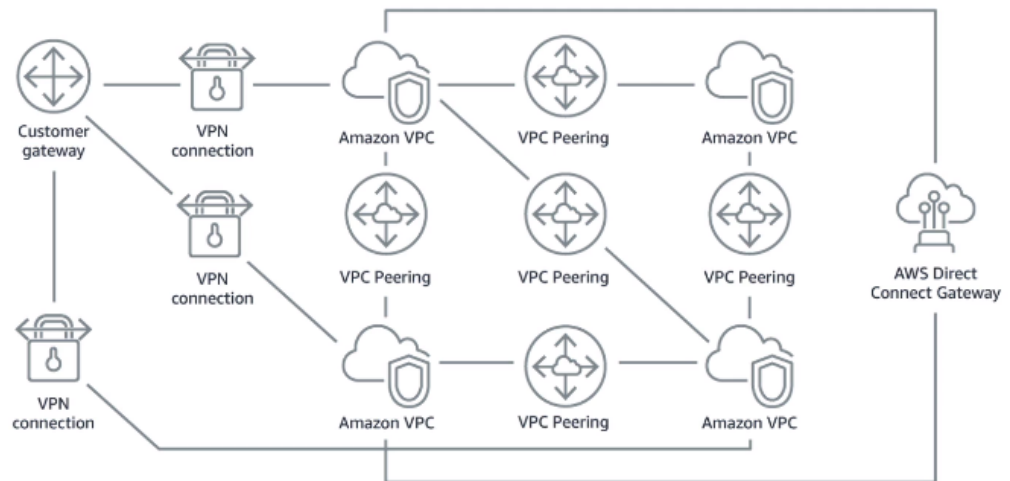
To use AWS Client VPN, you need to install the AWS Client VPN app on your device. Once you have installed the app, you can connect to your AWS resources using the app's user interface.

Here are some of the benefits of using AWS Client VPN:

- **Secure:** AWS Client VPN uses IPsec to encrypt all traffic between your device and your AWS resources. This ensures that your traffic is secure even if you are connecting to a public Wi-Fi network.
- **Easy to use:** The AWS Client VPN app is easy to install and use. You can connect to your AWS resources using the app's user interface.

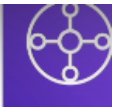
2.

Network topologies can become complicated

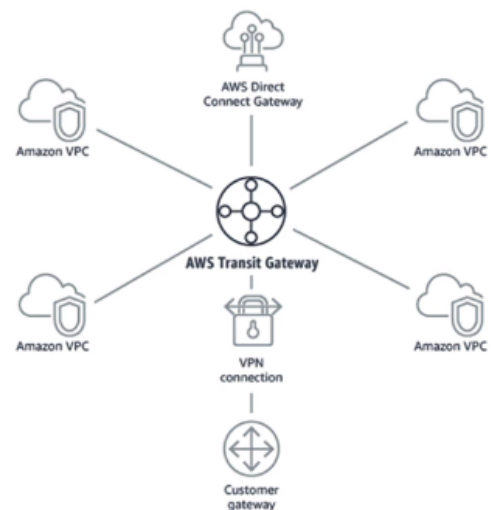


- 1.
2. If we too many networks,VPN's..it will get complicated

Transit Gateway



- For having transitive peering between thousands of VPC and on-premises, hub-and-spoke (star) connection
- One single Gateway to provide this functionality
- Works with Direct Connect Gateway,VPN connections



- 3.
4. So when in the exam, you see a way to connect hundreds or thousands of VPC together, with as well your on-premise infrastructure, think no more than the Transit Gateway.

VPC Closing Comments

- VPC: Virtual Private Cloud
- Subnets: Tied to an AZ, network partition of the VPC
- Internet Gateway: at the VPC level, provide Internet Access
- NAT Gateway / Instances: give internet access to private subnets
- NACL: Stateless, subnet rules for inbound and outbound
- Security Groups: Stateful, operate at the EC2 instance level or ENI
- VPC Peering: Connect two VPC with non overlapping IP ranges, nontransitive

1.

- Elastic IP –fixed public IPv4, ongoing cost if not in-use

2.

VPC Closing Comments

- VPC Endpoints: Provide private access to AWS Services within VPC
- PrivateLink: Privately connect to a service in a 3rd party VPC
- VPC Flow Logs: network traffic logs
- Site to Site VPN: VPN over public internet between on-premises DC and AWS
- Client VPN: OpenVPN connection from your computer into your VPC
- Direct Connect: direct private connection to AWS
- Transit Gateway: Connect thousands of VPC and on-premises networks together

3.