









If you are studying for AWS Developer Associate Exam, this guide will help you with quick revision before the exam. it can use as study notes for your preparation.

Dashboard

Other Certification Notes

VPC

- VPC
- VPC And Subnets Primer
- Internet Gateway And NAT Gateways
- Network ACL And Security Groups
- Network ACLs vs Security Groups
- VPC Flow Logs
- VPC Peering
- VPC Endpoints
- Site to Site VPN \& Direct Connect
- VPC Summary

VPC And Subnets Primer

- VPC: 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.
- Public Subnets usually contain:
- o Load Balancers
- Static Websites
- Files
- Public Authentication Layers
- Private Subnets usually contain:
- Web application servers
- Databases
- Public and Private subnets can communicate if they're in the same VPC

Internet Gateway And 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

Network ACL And Security Groups

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

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)

Reference

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Security.html#VPC_Security_Comparison

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
- o 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

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)

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 • **Only used within your VPC**

Site to Site VPN & Direct Connect

- Site to Site VPN
- o Connectanon-premisesVPNtoAWS
- The connection is automatically encrypted
- Goes over the public internet
- Direct Connect (DX)
- o Establish a physical connection between on-premises and AWS
- $\circ\;$ The connection is private, secure and fast
- o Goes over a private network
- o Takes at least a month to establish
- Note: Site-to-site VPN and Direct Connect cannot access VPC endpoints

VPC Summary

- 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
- $\bullet\;$ VPC Peering: Connect two VPC with non overlapping IP ranges, non transitive
- VPC Endpoints: Provide private access to AWS Services with
- VPC Flow Logs: network traffic logs
- Site to Site VPN: VPN over public internet between on-premises DC and AWS Direct Connect: direct private connection to a AWS