**Section 6:----VPC Fundamentals**

Machine generated alternative text:
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 Developer Level, you should know about: 
• VPC, Subnets, Internet Gateways & NAT Gateways 
• Security Groups, NetworkACL (NACL),VPC Flow Logs 
• VPC Peering VPC Endpoints 
• Site to Site VPN & Direct Connect 
• I will just give you an overview, less than I or 2 questions at your exam. 
• Later in the course, I will be highlighting when VPC concepts are helpful 

**VPC ,Subnets,IGW and NAT**

Machine generated alternative text:
VPC & Subnets Primer 
• VPC: private network to deploy your 
resources (regional resource) 
• Subnets allow you to partition your 
network inside yourVPC 
(Availability Zone resource) 
• A public subnet is a subnet that s 
accessible from the internet 
• A private subnet is a subnet that is 
accessible from the internet 
• To define access to the internet and 
between subnets, we use Route Tables. 
Public Subnet 
Private Subnet 
AZ A 

**NOTE:**

one ec2 instance in public subnet that is accessible by internet and other one in

Private subnet that is not accessible by internet

**High level diagram**

Machine generated alternative text:
VPC Diagram 
aws 
AWS aoud 
Availability Zone 1 
Region 
VPCCtDRRange: 
0.0. 0/16 
Availability Zone 2 
Public subnet 

**Ec2 in public subnet and it will route using IGW and it know how to talk with internet**

Machine generated alternative text:
Internet Gateway & NAT Gateways 
IGW 
NAT 
• Internet Gateways helps ourVPC 
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 
Public Subnet 
o 
Private Subnet 
AZ A 

**Private subnet will access by nat and nat connect to IGW**

Network Address Translation (**NAT**) Gateway, a highly available **AWS** managed service that makes it easy to connect to the Internet from instances within a private subnet in an **AWS** Virtual Private Cloud (VPC). Previously, you needed to launch a **NAT** instance to enable **NAT** for instances in a private subnet.

**NACL ,SG, VPC flow logs**

NACL (Network access control list)

SG (security group)

VPC(virtual private cloud)

Machine generated alternative text:
Network ACL & Security Groups 
• NACL (Network ACL) 
• A firewall which controls traffc 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 traffc to and from an 
ENI / an EC2 Instance 
• Can have only ALLOW rules 
• Rules include IP addresses and other security 
groups 
Public subnet 
NACL 
Security group 

Before the traffic reaches to public subnet it has to pass through NACL which act as firewall

Machine generated alternative text:
Network ACLs vs Security Groups 
Security Group 
Operates at the instance level 
Supports allow rules only 
Is stateful: Return traffic is automatically allowed, 
regardless of any rules 
We evaluate all rules before 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 
Network ACL 
Operates at the subnet level 
Supports allow rules and deny rules 
Is stateless: Return traffic must be explicitly 
allowed by rules 
We process rules in number order when 
deciding whether to allow traffic 
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) 

Machine generated alternative text:
VPC Flow Logs 
• Capture information about IP traffc going into your interfaces: 
• VPC Flow Logs 
• Subnet Flow Logs 
• Elastic Netvvork 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 

VPC Peering, Endpoint, VPN ,DX

Two different region or two different account connect with each other

Machine generated alternative text:
VPC Peering 
• Connect twoVPC, 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 A 
VPC peering 
VPC peering 
VPCC 
VPCB 
VPC peering 

Machine generated alternative text:
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 yourVPC 
VPC 
Private subnet 
VPC Endpoint 
Interface (ENI) 
VPC Endpoint 
Gateway 
CloudWatch 
DynamoDB 

NOTE : to privately connect AWS service : will need to use Endpoint

Machine generated alternative text:
Site to Site VPN & Direct Connect 
Public www 
Site-to-Site VPN 
(encrypted) 
VPC 
Private 
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 
Public 
On-premises DC 
Private 

VPC cheatsheet and closing comment

NOTE:

one default VPS is there per AWS region

Subnet : launching ec2 instance

Machine generated alternative text:
PC 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 intern 
s to private subnets 
• NACL: Stateless, subnet rules for in o utbound 
• Security Groups: Stateful, operate thq; —2 i stance level or ENI 
• VPC Peering: Connect two VPC wit ono apping IP ranges, non transitive 
• VPC Endpoints: Provide private access to AWS Services within VPC 
• VPC Flow Logs: network traffic logs 
• Site to SiteVPN: VPN over public internet between on-premises DC and AWS 
to a AWS 
231 people have written a note here. 

Three tier architecture

Machine generated alternative text:
Typical 3 tier solution architecture 
ElastiCache 
Store / retrieve 
session data 
+ Cached data 
Amazon RDS 
Read / write data 
Route 53 
53 
WIti AZ 
ELB 
Auto E ing group 
zone I 
Availability zone 2 
Availability Zone 3 
MS 
PRIVATE 

Machine generated alternative text:
LAMP Stack on EC2 
• Linux: OS for EC2 instances 
• Apache: Web Server that run on Linux (EC2) 
• MySQL: database on RDS 
• PHP:Application logic (running on EC2) 
• Can add Redis / Me cached (ElastiCac e) to include a caching tech 
• To store local applic ion data & softwa : EBS drive (root) 

Machine generated alternative text:
WordPress on AWS (more complicated) 