* Networking - VPC *

- /28 means 16 IPs (= 2^ (^{3}~~28-~~ 32-28) = 2^4) means only the last digit can change.
- CIDR not should overlap, and max CIDR size in AWS is /16.
- Subnet size: /26 = 64 IPs
- Security groups operate at the EC2 instance level while NACLs operate at the Subnet level.
- Security groups are stateful and if traffic can go out, then it can go back in.
- NAT Gateway: Least amount of administration and scales seamlessly.
- Route tables must be updated in both VPCs that are peered.
- Access VPC in another AWS region from your corporate datacenter: Use a Direct Connect Gateway.

Scanned with CamScanner

- Only Amazon S3 & DynamoDB are the two services have a VPC Gateway Endpoint, all the other services have an interface endpoint (powered by Private Link - means a private IP)
- VPC Flow logs is a VPC feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC
- A Dedicated Direct Connect connection supports 1 Gbps and 10 Gbps.
- Hosted Direct connect connection supports 50Mbps, 500Mbps upto 10Gbps.
- AWS Site-to-Site VPN connection between your corporate on-premises datacenter and VPCs in AWS cloud : Two major compounts to configure for this connection - Virtual Private Gateway and Customer gateway.
- Dedicated connection between your on-premises corporate datacenter and AWS Cloud; connection must be private, consistent and traffic must not travel through the internet : Use AWS Direct Connect
- Using a Direct Connect connection, you can access both public & private AWS resources.
- Scale up an AWS site-to-site VPN connection throughput, established between your on-premise

data and AWS cloud, beyond a single IPsec tunnel's max. limit of 1.25 Gbps: use Transit Gateway.

- Best configuration for bastion host Security Group to make it secure: Allow traffic only on port 22 from the company's public CIDR.
- Cost-effective secure backup connection in case there are issues with this Direct Connect connection: Setup a site-to-site VPN connection as a backup
- AWS Network Firewall: AWS service allows you to protect and control traffic in your VPC from layer 3 to layer 7.