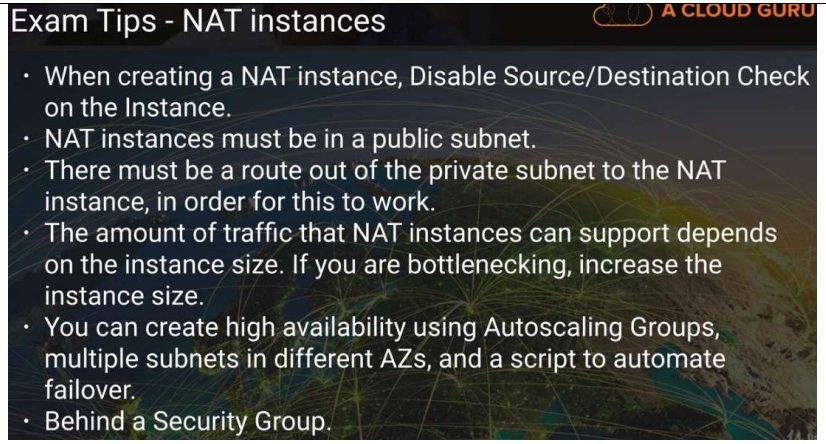
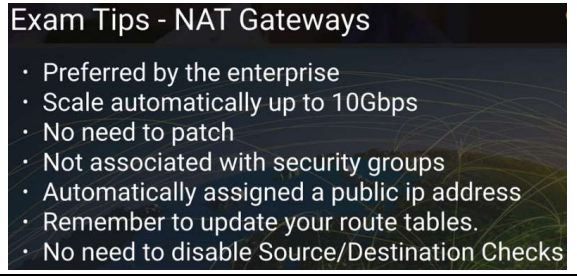
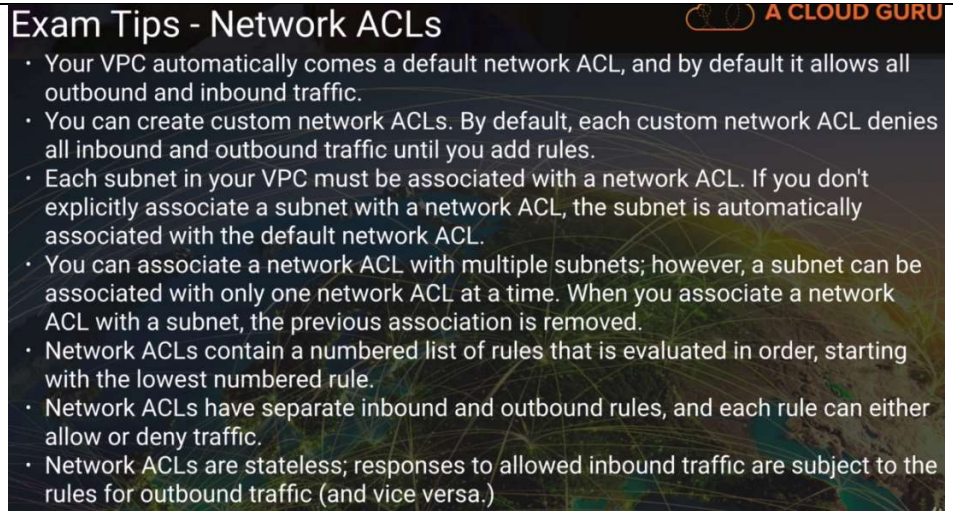
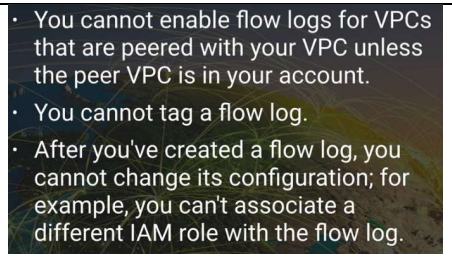
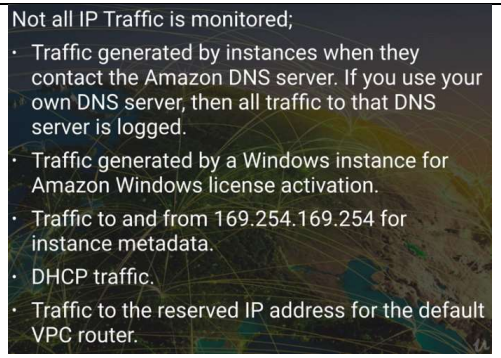
VPC Overview	CIDR.xyz VPC as a logical datacenter in AWS. Consists of IGWs (or Virtual Private Gateways), Route Tables, Network Access Control Lists, Subnets, and Security Groups. 1 Subnet = 1 Availability Zone Security Groups are **Stateful** and Network Access Control Lists are **Stateless**. **Stateful** - If you open port 80 of your security group, automatically you can both send and receive port 80. **Stateless** – You have to both open inbound and outbound ports.
NAT Instances & Nat Gateways	 
NAT vs Bastions	▪ A NAT is used to provde internet traffic to EC2 instances in private subnets. ▪ A Bastion is used to securely administer EC2 instances (using SSH or RDP) in private subnets.

Network ACLs	
VPC Endpoint for S3	These endpoints are easy to configure, highly reliable, and provide a secure connection to S3 that does not require a gateway or NAT instances. EC2 instances running in private subnets of a VPC can have controlled access to S3 buckets, objects, and API functions that are in the same region as the VPC. You can use an S3 bucket policy to indicate which VPCs and which VPC Endpoints have access to your S3 buckets.
VPC Flow Logs	

	 Not all IP Traffic is monitored; • Traffic generated by instances when they contact the Amazon DNS server. If you use your own DNS server, then all traffic to that DNS server is logged. • Traffic generated by a Windows instance for Amazon Windows license activation. • Traffic to and from 169.254.169.254 for instance metadata. • DHCP traffic. • Traffic to the reserved IP address for the default VPC router.	