

VPC Overview	<p>CIDR.xyz</p> <p>VPC as a logical datacenter in AWS.</p> <p>Consists of IGWs (or Virtual Private Gateways), Route Tables, Network Access Control Lists, Subnets, and Security Groups.</p> <p>1 Subnet = 1 Availability Zone</p> <p>Security Groups are Stateful and Network Access Control Lists are Stateless.</p> <p>Stateful - If you open port 80 of your security group, automatically you can both send and receive port 80.</p> <p>Stateless – You have to both open inbound and outbound ports.</p>
NAT Instances & Nat Gateways	<div data-bbox="516 493 1320 927"> <p>Exam Tips - NAT instances</p> <ul style="list-style-type: none"> • When creating a NAT instance, Disable Source/Destination Check on the Instance. • NAT instances must be in a public subnet. • There must be a route out of the private subnet to the NAT instance, in order for this to work. • The amount of traffic that NAT instances can support depends on the instance size. If you are bottlenecking, increase the instance size. • You can create high availability using Autoscaling Groups, multiple subnets in different AZs, and a script to automate failover. • Behind a Security Group. </div> <div data-bbox="516 927 1073 1198"> <p>Exam Tips - NAT Gateways</p> <ul style="list-style-type: none"> • Preferred by the enterprise • Scale automatically up to 10Gbps • No need to patch • Not associated with security groups • Automatically assigned a public ip address • Remember to update your route tables. • No need to disable Source/Destination Checks </div>
NAT vs Bastions	<ul style="list-style-type: none"> ▪ A NAT is used to provide 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	<div data-bbox="516 250 1451 792"> <h3>Exam Tips - Network ACLs</h3> <ul style="list-style-type: none"> • Your VPC automatically comes a default network ACL, and by default it allows all outbound and inbound traffic. • You can create custom network ACLs. By default, each custom network ACL denies all inbound and outbound traffic until you add rules. • Each subnet in your VPC must be associated with a network ACL. If you don't explicitly associate a subnet with a network ACL, the subnet is automatically associated with the default network ACL. • You can associate a network ACL with multiple subnets; however, a subnet can be associated with only one network ACL at a time. When you associate a network ACL with a subnet, the previous association is removed. • Network ACLs contain a numbered list of rules that is evaluated in order, starting with the lowest numbered rule. • Network ACLs have separate inbound and outbound rules, and each rule can either allow or deny traffic. • Network ACLs are stateless; responses to allowed inbound traffic are subject to the rules for outbound traffic (and vice versa.) <p>• Block IP Addresses using network ACLs not Security Groups</p> </div>
VPC Endpoint for S3	<p>These endpoints are easy to configure, highly reliable, and provide a secure connection to S3 that does not require a gateway or NAT instances.</p> <p>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.</p>
VPC Flow Logs	<ul style="list-style-type: none"> • You cannot enable flow logs for VPCs that are peered with your VPC unless the peer VPC is in your account. • You cannot tag a flow log. • After you've created a flow log, you cannot change its configuration; for example, you can't associate a different IAM role with the flow log.

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.