A CLOUD GURU

VPC Summary

Ryan Kroonenburg
AWS COMMUNITY HERO & ALEXA CHAMPION
FOUNDER OF A CLOUD GURU

Remember the following;

- Think of a 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; Network Access Control Lists are Stateless
- NO TRANSITIVE PEERING

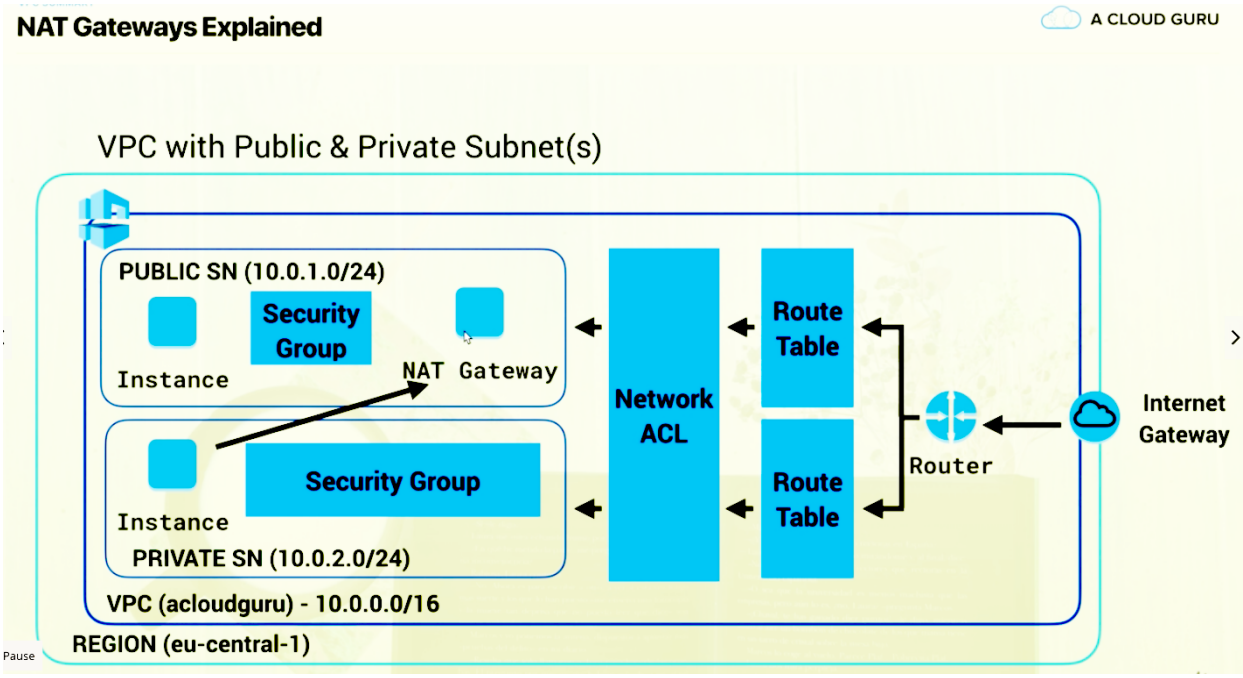
Security Group: Open port, don't need to worry about outbound traffic, it's automatic
NACL: Do inbound and outbound

Remember the following;

- When you create a VPC a default Route Table, Network Access Control List (NACL) and a default Security Group.
- It won't create any subnets, nor will it create a default internet gateway.
- US-East-1A in your AWS account can be a completely different availability zone to US-East-1A in another AWS account. The AZ's are randomized.
- Amazon always reserve 5 IP addresses within your subnets.
- You can only have 1 Internet Gateway per VPC.
- Security Groups can't span VPCs.

Nat Instances Exam Tips

- 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.



Nat Gateways

- Redundant inside the Availability Zone
- Preferred by the enterprise
- Starts at 5Gbps and scales currently to 45Gbps
- 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

Nat Gateways

- If you have resources in multiple Availability Zones and they share one NAT gateway, in the event that the NAT gateway's Availability Zone is down, resources in the other Availability Zones lose internet access. To create an Availability Zone-independent architecture, create a NAT gateway in each Availability Zone and configure your routing to ensure that resources use the NAT gateway in the same Availability Zone.

Network ACL's

Remember the following for your exam;

- Your VPC automatically comes with 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.
- Block IP Addresses using network ACLs not Security Groups.

VPC SUMMARY

Network ACL's

Remember the following for your exam;

- 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.)

VPC SUMMARY

ELB's And VPCs

Remember the following for your exam;

- You need a minimum of two public subnets to deploy an internet facing loadbalancer.

VPC SUMMARY

VPC Flow Logs

Remember the following;

- You cannot enable flow logs for VPCs that are peered with your VPC unless the peer VPC is in your account.
- You can tag flow logs.
- 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.

VPC SUMMARY

VPC Flow Logs

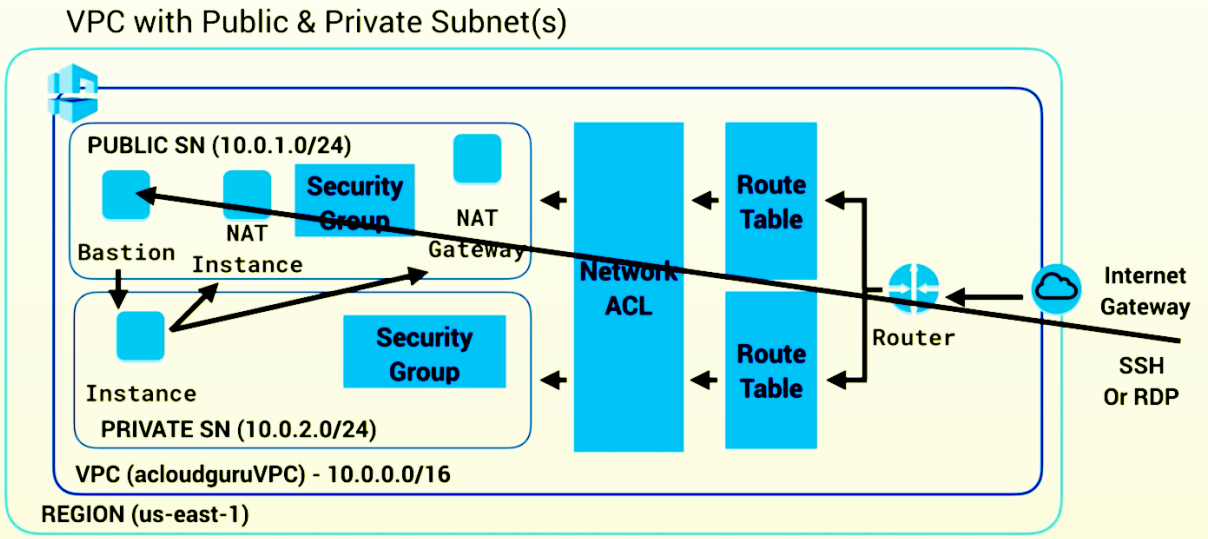
Not all IP Traffic is monitored;

- 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.

VPC SUMMARY

Bastions In Action

A CLOUD GURU



VPC SUMMARY

Bastions vs NAT Gateways/Instances

Remember the following;

- A NAT Gateway or NAT Instance is used to provide internet traffic to EC2 instances in a private subnets.
- A Bastion is used to securely administer EC2 instances (Using SSH or RDP). Bastions are called Jump Boxes in Australia.
- You cannot use a NAT Gateway as a Bastion host.

VPC SUMMARY

Direct Connect

Remember the following;

- Direct Connect directly connects your data center to AWS
- Useful for high throughput workloads (ie lots of network traffic)
- Or if you need a stable and reliable secure connection.

SETTING UP DIRECT CONNECT

Direct Connect - Exam Tips

Remember the Steps to Creating a Direct Connect Connection.

- Create a virtual interface in the Direct Connect console. This is a PUBLIC Virtual Interface.
- Go to the VPC console and then to VPN connections. Create a Customer Gateway.
- Create a Virtual Private Gateway
- Attach the Virtual Private Gateway to the desired VPC.
- Select VPN Connections and create new VPN Connection.
- Select the Virtual Private Gateway and the Customer Gateway
- Once the VPN is available, setup the VPN on the customer gateway or firewall.

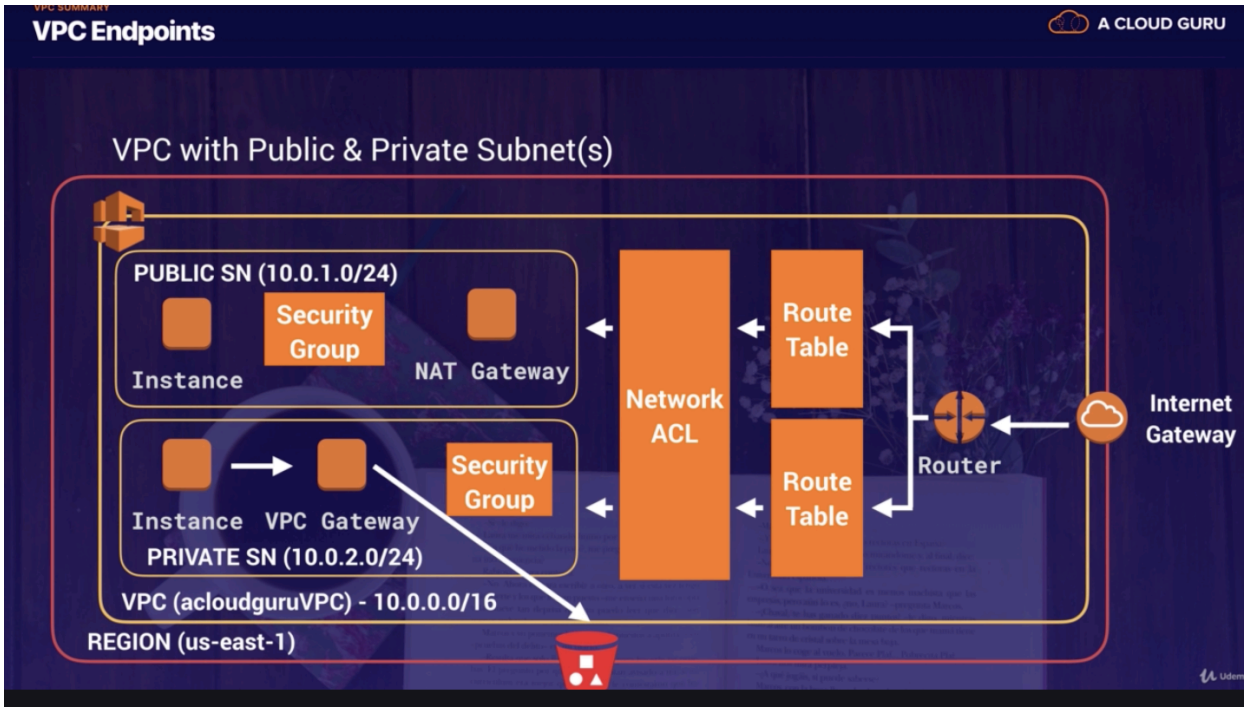
Know what a Global Accelerator is and where you would use it.

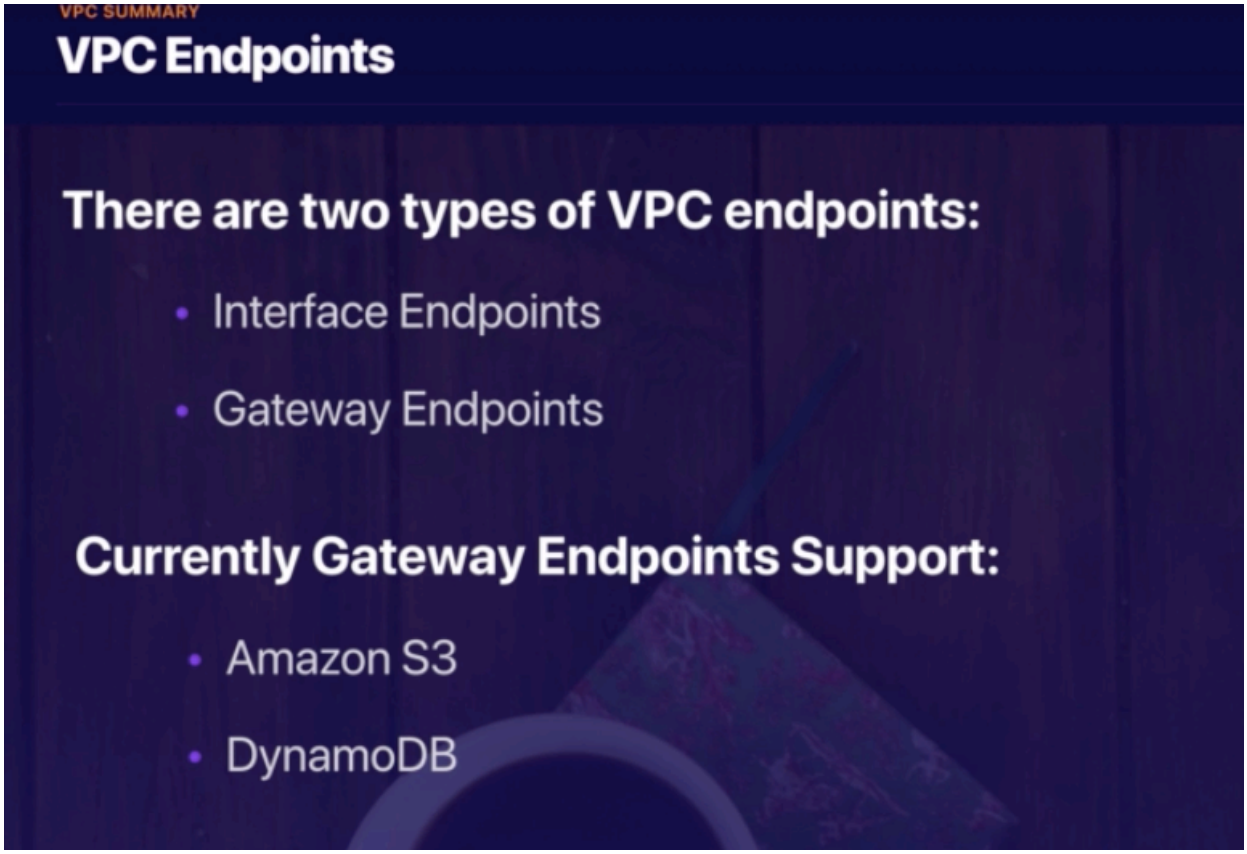
- AWS Global Accelerator is a service in which you create accelerators to improve availability and performance of your applications for local and global users.
- You are assigned two static IP addresses (or alternatively you can bring your own).
- You can control traffic using traffic dials. This is done within the endpoint group.
- You can control weighting to individual end points using weights.

A VPC Endpoint:

A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC do not require public IP addresses to communicate with resources in the service. Traffic between your VPC and the other service does not leave the Amazon network.

Endpoints are virtual devices. They are horizontally scaled, redundant, and highly available VPC components that allow communication between instances in your VPC and services without imposing availability risks or bandwidth constraints on your network traffic.


VPC SUMMARY
VPC Endpoints
A CLOUD GURU
VPC with Public & Private Subnet(s)
PUBLIC SN (10.0.1.0/24)
Security Group
Instance
NAT Gateway
Network ACL
Route Table
Route Table
Router
Internet Gateway
Security Group
Instance
VPC Gateway
PRIVATE SN (10.0.2.0/24)
VPC (acloudguruVPC) - 10.0.0.0/16
REGION (us-east-1)


VPC SUMMARY
VPC Endpoints
There are two types of VPC endpoints:
• Interface Endpoints
• Gateway Endpoints
Currently Gateway Endpoints Support:
• Amazon S3
• DynamoDB