# VPC

Important section for all exams☺. You should be able to build out your own VPCs from memory.

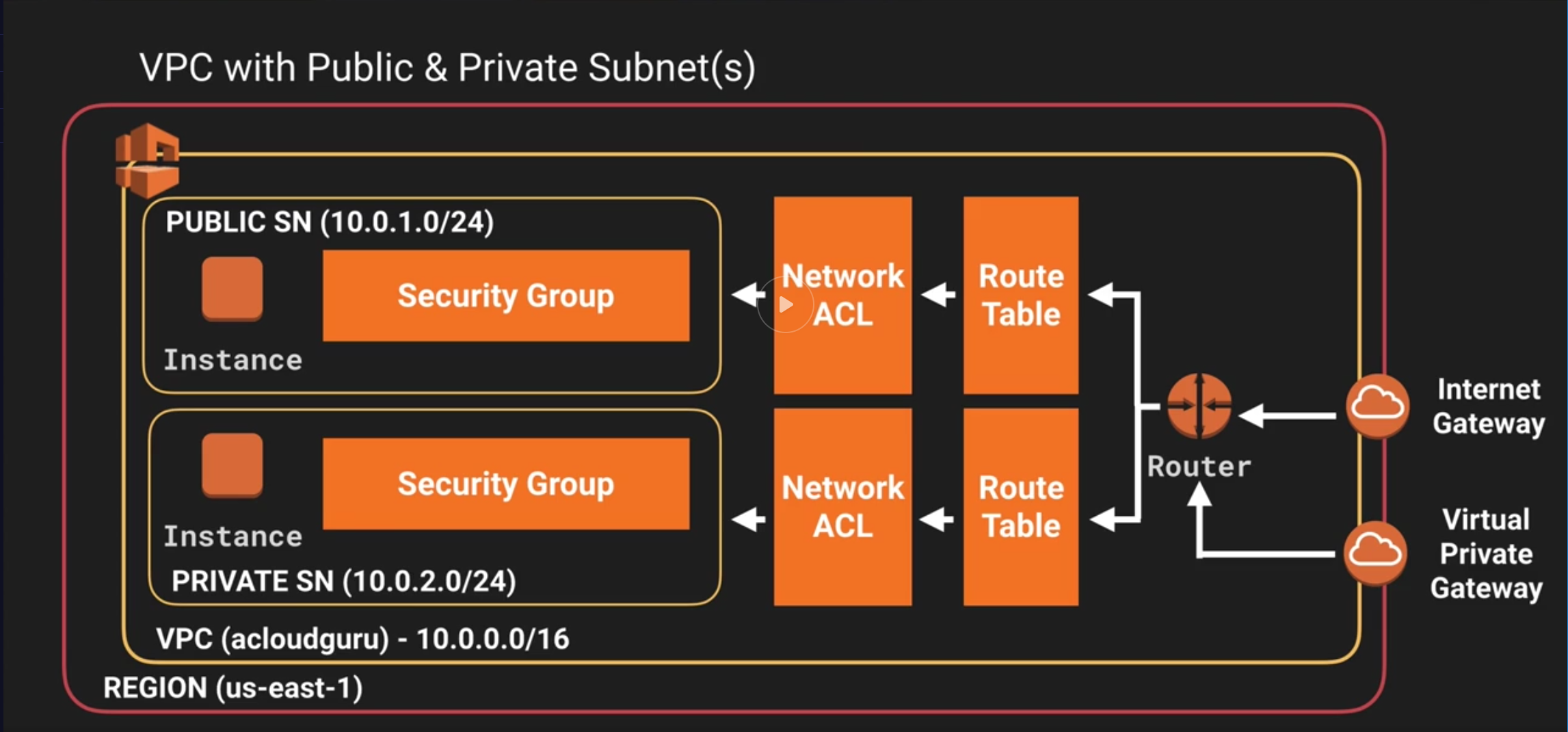
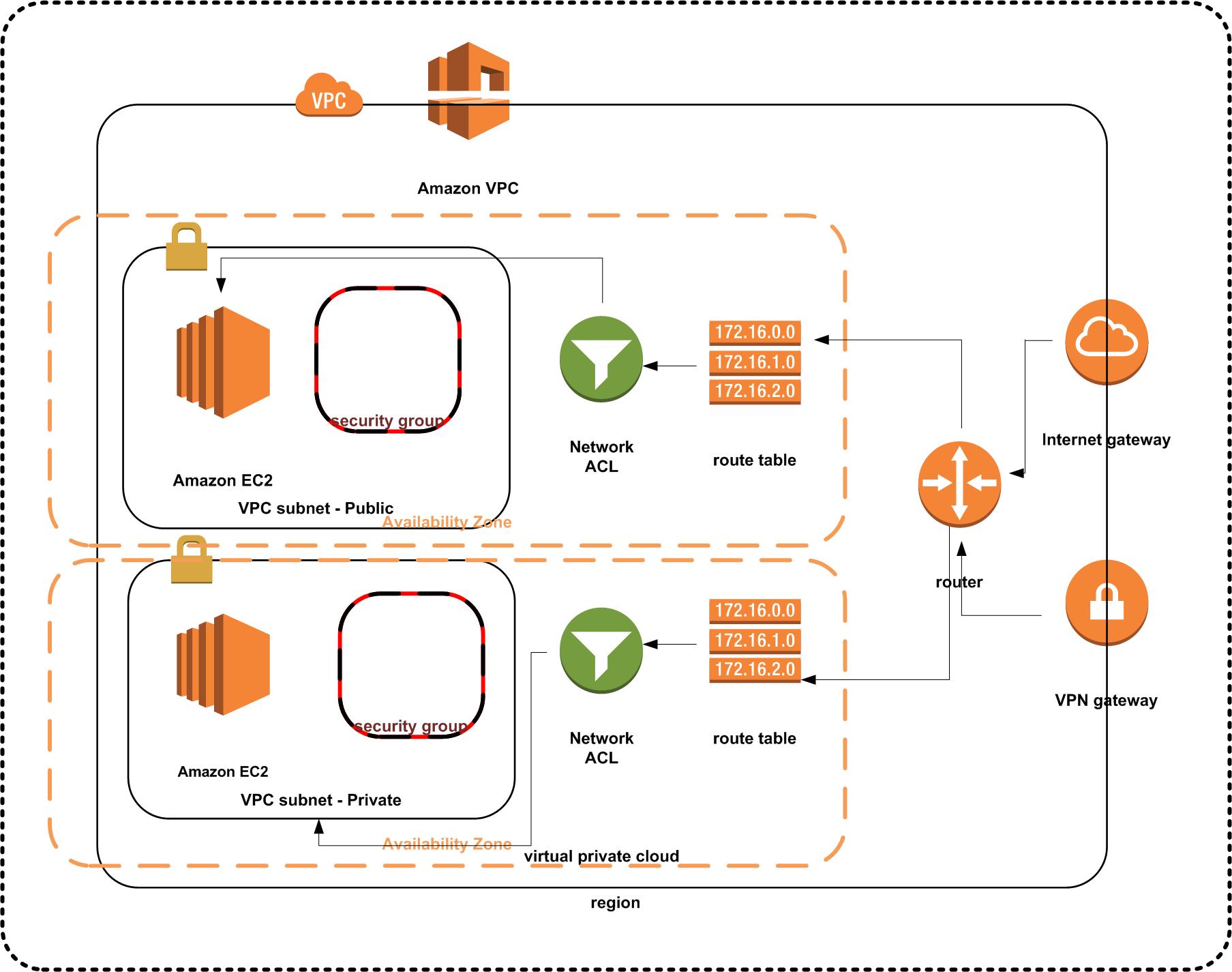
* VPC is a logical data center within an AWS Region.
* Control over network environment, select IP address range, subnets and configure route tables and gateways.
* VPC Do not span regions, but can span AZs
* Hardware Virtual Private Network (VPN) connection between your corporate datacenter and your VPC and thus extend your own data center.
* Can create public facing subnet (Web) having internet access and private facing subnet (DB) with no internet access
* Public Subnet – Web Servers/ Jump Boxes
* Private Subnet – Applications Servers / Database servers
* Leverage multiple layers of security – Security groups and Network ACLs to control access to EC2 instances
* Create hardware VPN connection between your local DC and AWS.
* AWS gives a maximum of /16 network.
* To change VPC addressing, you have to drop and recreate the VPC
* Bastion host/ Jump Box in Public subnet
* **VPC Consists of**
  + **Internet Gateway** connect to internet for public subnet and is scaled, redundant and highly available. (1 per VPC)
  + **Subnets** – Do not span AZs
  + **NACL**:
    - Control traffic to and from subnets.
    - Stateless
    - Span AZs
    - Can use both Allow and Deny rules
    - A subnet can be associated with 1 NACL at a time
  + **Security Groups**:
    - Control Traffic to and from Instances.
    - Stateful
    - Span AZs
  + **Route Tables – (Span AZs)**
  + **NAT Gateway** – connect to internet for private subnet
  + **Virtual Private Gateway**: The Amazon VPC side of a VPN connection.
  + **Customer Gateway**: The customer side of a VPN connection.
  + **Peering Connection**: A peering connection enables you to route traffic via private IP addresses between two peered VPCs.
    - Peering may be between VPCs in same or different accounts
    - No Transitive Peering. Point to Point only
    - Can peer only with VPCs in the same region
    - Must have non-overlapping address ranges
    - Peering traffic is not encrypted
  + **VPC Endpoint**: Enables Amazon S3 access from within your VPC without using an Internet gateway or NAT.
  + **ElasticIP**: Public Routable IP Address for inbound traffic
* By default, how many VPCs am I allowed in each AWS Region? == 5
* *Can Amazon EC2 instances within a VPC in one region communicate with Amazon EC2 instances within a VPC in another region?* Yes, they can communicate using public IP addresses, NAT gateway, NAT instances, VPN connections, or Direct Connect connections.
* You can use AMIs in Amazon VPC that are registered within the same region as your VPC
* Amazon Virtual Private Cloud (VPC) ClassicLink allows EC2 instances in the EC2-Classic platform to communicate with instances in a VPC using private IP addresses.
* An instance launched in a VPC using an Amazon EBS-backed AMI maintains the same IP address when stopped and restarted.
* *Can I have more than two network interfaces attached to my EC2 instance?* – Yes, The total number of network interfaces that can be attached to an EC2 instance depends on the instance type
* Network interfaces can only be attached to instances residing in the same Availability Zone
* Ping (ICMP Echo Request and Echo Reply) requests to the router in your VPC is not supported. Ping between Amazon EC2 instances within VPC is supported as long as your operating system's firewalls, VPC security groups, and network ACLs permit such traffic.
* Primary private IP addresses are retained for the instance's or interface's lifetime. Secondary private IP addresses can be assigned, unassigned, or moved between interfaces or instances at any time.
* An IP address assigned to a running instance can only be used again by another instance once that original running instance is in a "terminated" state.
* The number of secondary private IP addresses you can assign depends on the instance type.
* AWS VPC does not support multicast or broadcast

Typical Private IP address ranges – not publicly routable.

* 10.0.0.0 - 10.255.255.255 (10/8 prefix)
* 172.16.0.0 - 172.31.255.255 (172.16/12 prefix) – Default VPC
* 192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

VPC Diagram - Public and Private subnets

* Internet Gateway/Virtual Private gateway 🡪Via Router table 🡪 NACL🡪 Security Group 🡪 Instance

[](https://github.com/agasthik/aws-csa-2017/blob/master/VPC-Diagram.jpg)

To use AWS Stencils download them at the [AWS Simple Icons for Architecture Diagrams](https://aws.amazon.com/architecture/icons/) site

## Default v/s Custom VPC

* When you create an account a default VPC is created for you in each Region.
* All subnets in default VPC have a route out to the internet
* Each EC2 instance in default VPC will have a public and private IP address

## Custom VPC Info

* Default Security group, network ACL & route table are created for each custom VPC you create.
* Doesn’t create subnets or internet gateways out of the box.
* In each VPC you create, 5 IP addresses are reserved by AWS for itself. First 4 and last IP in the CIDR block.
* You can't change the size of a VPC after you create it. If your VPC is too small to meet your needs, create a new, larger VPC, and then migrate your instances to the new VPC. To do this, create AMIs from your running instances, and then launch replacement instances in your new, larger VPC. You can then terminate your old instances, and delete your smaller VPC.
* You can’t attach multiple Internet Gateways to the VPC to boost performance.
* When creating VPCs do not modify default route table to add your custom rules. If you modify the default route, it will affect all instances. Create a new route table for customization.

## NAT Instance & NAT Gateway

* NAT Instance is one EC2 instance. You are responsible for performance management, scale out and security groups. NAT Gateway is a managed service.
* On NAT instance, **remember to disable source/destination IP check**. This is required to allow private subnet internet connectivity. This is not required on NAT Gateway.
* Allow both HTTP and HTTPS access on security groups associated with NAT instances. Security groups are always associated with NAT Instances.
* **Both NAT Instance and NAT Gateways are deployed to public subnet**. Elastic IP has to be added to NAT Instance. NAT Gateway is automatically assigned a public IP.
* In VPC, update default route table to **allow connectivity from Private subnet to NAT Instance** and Gateway
* NAT instance is single point of failure. You can place NAT instance behind Auto Scaling group, multiple subnets in different AZs and scripted failover. To improve performance, increase the size of the NAT instance to allow for higher throughput.
* You can use Network ACLs to control traffic for both NAT Instance and Gateway.
* **NAT Gateways scale up to 10Gbps**. No need to disable source/ destination checks on Gateways.
* **Create NAT Gateways in multiple AZs for redundancy**
* NAT Gateways: IPv4 / Egress only NAT Gateway: IPv6

## Network ACLs & Security Groups

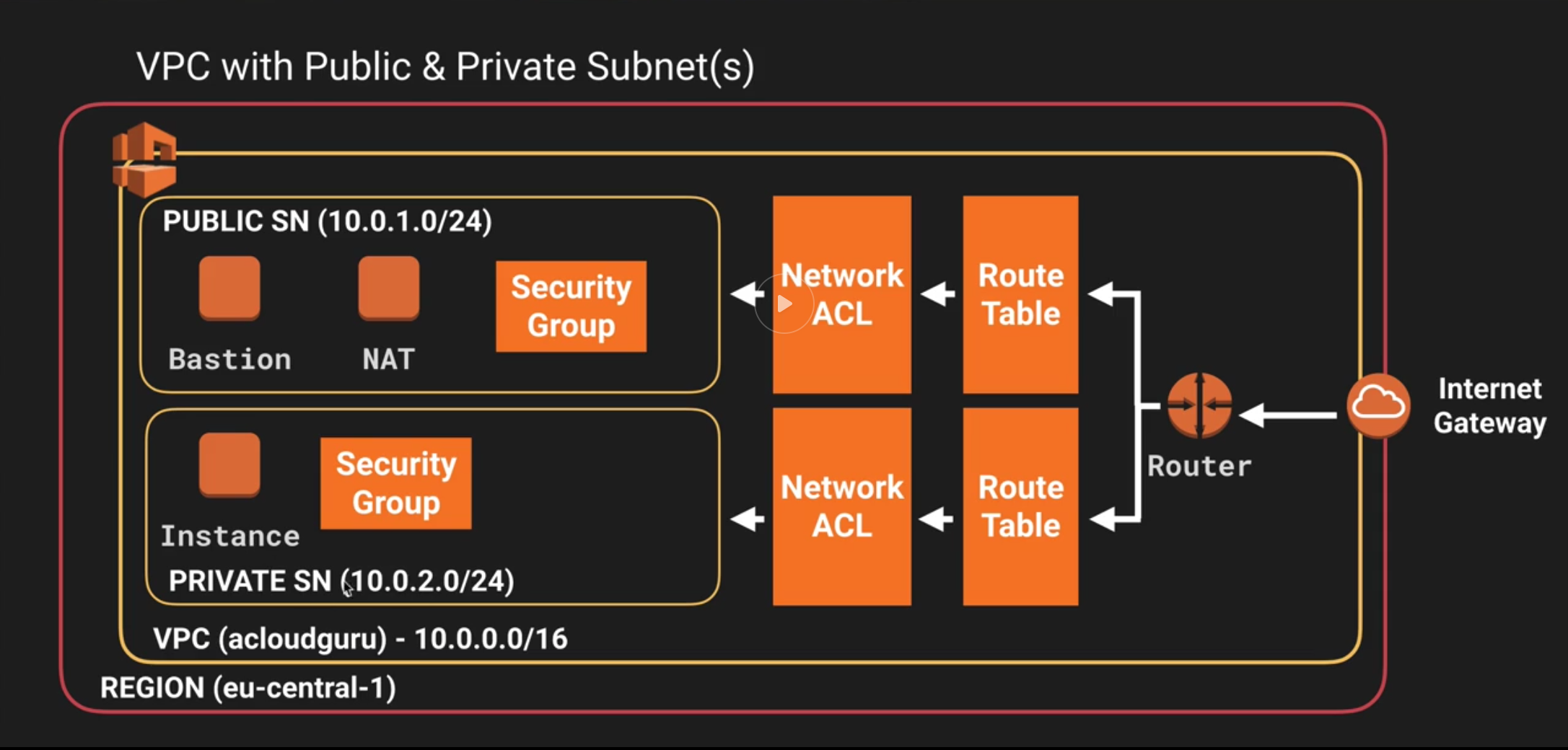
| **Security Group** | **Network ACL** |
| --- | --- |
| Operates at the instance level (first layer of defense) | Operates at the subnet level (second layer of defense) |
| Supports allow rules only | Supports allow rules and deny rules |
| Is stateful: Return traffic is automatically allowed, regardless of any rules | Is stateless: Return traffic must be explicitly allowed by rules |
| We **evaluate all rules before deciding** whether to allow traffic | We **process rules in number order** when deciding whether to allow traffic. Lower order rules take effect in case of conflict with higher order rules. |
| 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 | Automatically applies to all instances in the subnets it's associated with (backup layer of defense, so you don't have to rely on someone specifying the security group) |

* With default ACL, all inbound and outbound traffic is allowed automatically
* When custom ACL, all inbound and outbound traffic is denied by default
* 1 subnet <=> 1 AZ <=> 1 ACL. NACLs can be associated to only 1 subnet at a time. You can reassign to another subnet. If subnet is not associated with an ACL, the default ACL is applied.
* NACL can be associated with multiple subnets
* AWS Recommends adding ACL rules in increments of 100s
* Ephemeral ports – Allow inbound /outbound traffic from 1024 – 65535. As clients can initiate outbound connection from any random port. Ports < 1024 reserved for super user access.
* If you have to block a specific IP address / range, use ACLs instead of security groups. SGs can’t deny traffic – they only allow.

## Custom VPC & ELB

* To have HA in general or for ELB, ensure that you have at-least 2 public and or private subnets in different availability zones.

## NAT & Bastion



* You cannot use NAT instance to SSH / RDP into private subnet.
* Bastions are used for secure administrative tasks only. Bastions are placed in Public subnets and connect to private subnets via private IP
* For Bastion HA, have multiple Bastions in different AZs – at least 2 public subnets. Auto scaling in multiple AZ, route 53 doing health checks.
* NAT instance is used to provide internet connectivity to private subnets.

## VPC Flow Logs

* Enable Flow Logs for Custom VPC to see all traffic.
* Enable to capture IP traffic flow information for the NICs of your resources. All information is reported to CloudWatch
* Create IAM role to allow all logs to flow into CloudWatch
* Create log group in CloudWatch and inside that create stream where you can then see all the traffic flow
* You can only create flow logs for a VPC in the same account
* You cannot alter configuration of flow logs or tag it
* Flow logs are at 3 levels
  + VPC
  + Subnet
  + Network Interface
* Not Monitored:
  + Route 53 traffic
  + Windows license activation
  + 169.254.169.254 metadata
  + DHCP
  + Reserved IP address traffic

## VPC Endpoint

* By default, if you were to connect to a S3 bucket via NAT gateway, traffic would traverse the internet
* Endpoint creates a private network connection to S3
* Create Role 🡪 S3 Administrator
* EC2 🡪 Select Private --. Attach Role
* Ssh into private instance
* VPC 🡪 Endpoints 🡪 Create Endpoint 🡪 s3 Gateway 🡪 Policy
* Endpoints
  + Interface Endpoint: ENI entry point for traffic to Instance
  + Gateway endpoint: target for a route in your route table