VPC Notes

VPC is region specific and can extend between one or more Availablity Zones

One Subnet is confined to one Availability Zone…subnet cannot extend between two or more Availability Zones.

Components of VPC:

- CIDR and IP address subnets(10.0.0.0/8, 172.16.0.0/16, 192.168.0.0/16 – RFC 1918)
- Implied Router(for subnets to communicate with eachother)
- Route tables(Destination(ipaddress) & Target(IGW/local…etc)
- Internet gateway(to communicate with the outside the world)
- Security Groups(Virtual firewalls - last defence component in VPC – ENI/ NIC level)
- Network Access Contol List (First line of defence – Subnet level)
- Virtual Private Gateway(to connect to on premise servers)

Implied Router:

- It is central VPC routing function
- It connects the different AZ's together and connects the VPC to the Internet Gateway
- Each subnet will have a route table the route uses to forwarding traffic within the VPC
- The route tables will also have entries to external destinations

Route Tables:

- You can have upto 200 route tables per VPC
- You can have upto 50 routes entries per route table
- Each subnet must be associated with only one route table at any given time
- If you do not specify a subnet-to-route table association, the subnet(when created) will be associated with the main(default) VPC route table
- You can change the subnet association to another route table.
- One subnet can have only one route table where as one route table can be associated with multiple subnets.
- You can also edit the main(default) route table if you need, but you can not delete the main(default) route table. However, you can make a custom route table manually become the main route table, then you can delete the former main, as it is no longer a main route table.
- Every route table in VPC comes with a default rule that allows all VPC Subnets to communicate with one another. You cannot modify or delete this rule.

VPC IP Addressing:

- Once the VPC is created, you cannot change its CIDR block range
- Size of CIDR block that can be created is /28 - /16
- The different subnets within a VPC cannot overlap
- You can however, expand your VPC CIDR by adding new/extra IP

VPC Notes

AWS Reserved IP's in each subnet:

- Ex: If the subnet is 10.0.0.0/24
- 10.0.0.0 is the base network
- 10.0.0.1 VPC router
- 10.0.0.2 DNS related
- 10.0.0.3 Reserved for future use
- 10.0.0.255 last IP – broadcasrting

Internet Gateway:

- An internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between instances in your VPC and the internet. It therefore imposes no availability risks or bandwidth constraints on your network.
- You are charged for creating and using a NAT gateway in your account. NAT gateway hourly usage and data processing rates apply.
- It performs NAT(static one-to-one) between your private and public(or Elastic) IPv4 addresses
- It supports both IPv4 and IPv6

Public Subnet vs Private Subnet:

As per RFP1918:

- 10.0.0.0, 172.16.0.0 and 192.168.0.0 are private IPs

VPC Types:

1. Default VPC:
   Created in each AWS region when an AWS account is created
   Has default CIDR, Security Group, NACL and route table settings
   Has an Internet Gateway by default
   It allows all traffic Inbound(source) and Outbound(any)
2. A Custom VPC:
   Is a VPC an AWS account owner creates
   AWS user creating the custom VPC can decide the CIDR
   Has its own default Security Group, NACL and Route tables
   Does not have an Internet Gateway by default, one needs to be created if required
   Auto assign IPs is set to no for custom VPC by default, we can change it to Enable auto-assign public IPv4 address from the actions tab/dropdown

Security Groups:

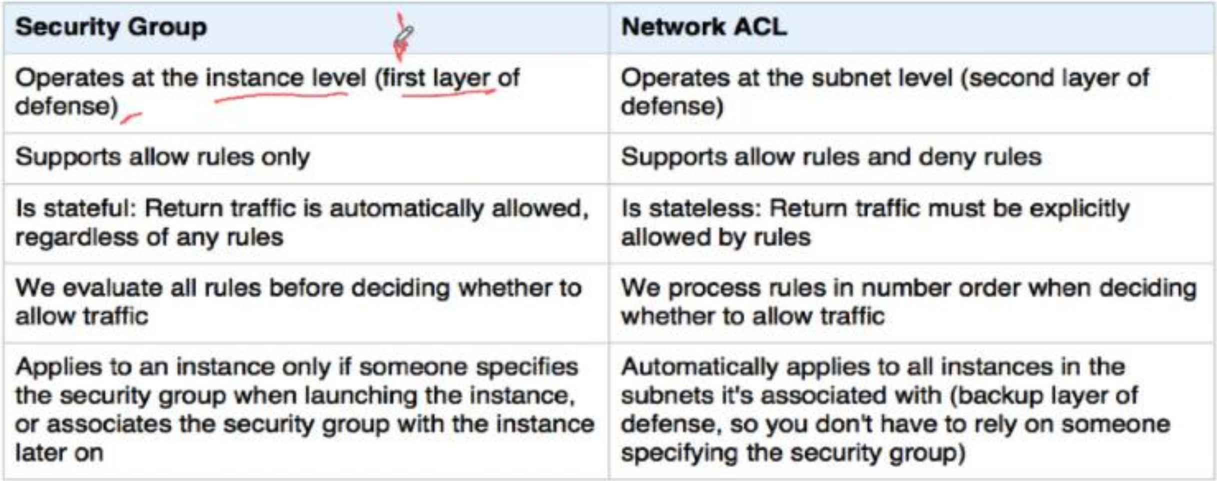
- A Security group is a virtual firewall
- Security Groups are STATEFULL, i.e whatever traffic is allowed for inbound all the traffic will be allowed outbound.
- It controls traffic at the virtual server (EC2 Instance) level – Specifically at the virtual Network Interface level
- Up to 5 security groups per EC2 instance interface can be applied

- Stateful, return traffic, of allowed inbound traffic, is allowed, even if there are no rules to allow it
- Can only have permit rules, cannot have deny rules
- Implicit deny rule at the end
- Security Groups are associated with EC2 instances network interfaces
- All rules are evaluated to find a permit rule
- VPC is region bound, VPC created in one region cannot be viewed in a different region.
- A custom Security group(newly created) will have all the rules implicitly deny for inbound, i.e we need to explicitly add the rules for inbound. However, everything is allowed for outbound by default.
- Each VPC created will have a default Security Group created for it, you cannot delete default Security group.
- Security groups are VPC resources, hence, different EC2 instances, in different Availability Zones, belonging to the same VPC, can have the same security group applied to them.
- Changes to Security groups take effect immediately
- **Default Security Group** in a default or custom VPC, will have:
  1. Inbound rules allowing instances assigned the same security group to talk to one another
  2. All outbound traffic is allowed
- **Custom(Non-default) Security groups** in a VPC will always have:
  1. No inbound rules – basically all inbound traffic is denied by default
  2. All outbound traffic is allowed by default
- Security groups are directional and can use allow rules only
- We cannot use subnet ID as source or destination for Security groups

NACL(Network Access Control Lists):

- It is a function performed on the implied router(The implied VPC router hosts the Network ACL function).
- It functions at the Subnet Level
- NACLs are **Stateless.** Outbound traffic for an allowed inbound traffic, must be "explicitly" allowed too
- You can have "permit" and "deny" rules in a NACL
- NACL is a set of rules, each has a number
- NACL rules are checked for a "permit" from lower numbered rules until either a permit is found or an explicit/implicit deny is reached
- You can insert rules(based on the configured rule number spacing) between existing rules, hence, it is recommended to leave a number range between any two rules to allow for edits later
- NACLs end with an explicit deny any, which you cannot delete
- A subnet must be associated with a NACL, if you do not specify the NACL, the subnet will get associated with the default NACL automatically
- You can create your own custom NACL, you do not have to use the default NACL
- **A default NACL allows all traffic inbound and outbound**
- **A custom(non-default) NACL blocks/denies all traffic inbound and outbound**

VPC Notes



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
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)

NAT Instance:

- The NAT instance is configured in a public subnet
- NAT instance need to be assigned a security group
- NAT instance is there to enable the private subnet EC2 instances to get to the internet
- No traffic initiated from the Internet can access the private subnet
- Only admin SSH traffic can be allowed to the NAT instance(or RDP if windows)
- Public subnet EC2 instances don’t need to go through NAT
- Private subnet EC2 instances need to access websites on the internet(HTTP or HTTPS)
- NAT instances security group must allow:
  1. Traffic inbound from the private subnet or the private subnet’s security group as a source on ports 80(HTTP) and 443(HTTPS)
  2. Traffic outbound to 0.0.0.0/0(internet) on ports 80 and 443
  3. Traffic inbound from the customer’s own network on port 22(SSH) to administer the NAT instance

NAT Gateway:

- Is an AWS managed service
- Cannot be assigned a security group
- AWS is responsible for its security/patching etc
- Works only with an Elastic IP, cannot use a public IP to do its function

VPC Peering:

- A VPC Peering connecting is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses
- Instances in either VPC can communicate with each other as if they are within the same network
- You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account within a single region or between regions(inter-region VPC peering)

- AWS uses the existing infrastructure of a VPC to create a VPC peering connection neither a gateway nor a VPN connection, and does not rely on a separate piece of physical hardware.
- There is no single point of failure for communication or a bandwidth bottleneck
- Examples of VPC peering connections usage:
    1. If you have more than one AWS account, you can peer the VPCs across those accounts to create a file sharing network
    2. You can use a VPC peering connection to allow other VPCs to access resources you have in one of your VPCs
- To establish a VPC peering connection, you do the following:
    1. The owner of the requester VPC(or local VPC) sends a request to the owner of the peer VPC to create the VPC peering connection. The peer VPC can be owned by you, or another AWS account, and cannot have a CIDR block that overlaps with the requester VPC's CIDR block
    2. The owner of the VPC accepts the VPC peering connection request to activate the VPC peering connection
    3. To enable the flow of traffic between the peer VPCs using private IP addresses, add a route to one or more of your VPC's route tables that points to the IP address range of the peer VPC. The owner of the peer VPC adds a route to one of their VPC route tables that points to the IP address range of your VPC.
    4. If required, update the security group rules that are associated with your instances to ensure that traffic to and from the peer VPC is not restricted
- A VPC peering connection is a one to one relationship between two VPCs. You can create multiple VPC peering connections for each VPC that you own
- Transitive peering relationships are not supported: you do not have any peering relationship with VPCs that your VPC is not directly peered with.

VPC Flow Logs:

VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC. Flow log data is stored using Amazon CloudWatch Logs. After you've created a flow log, you can view and retrieve its data in Amazon CloudWatch logs.

Flow logs can be created at 3 levels:

- VPC
- Subnet
- Network Interface level

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.

Direct Connect:

AWS Direct Connect is a cloud service solution that makes it easy to establish a dedicated network connection from your premises to AWS. Using AWS Direct connect, you can establish private connectivity between AWS and your datacenter, which in many cases can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than internet-based connection.

Elastic IP:

An Elastic IP address is a static IPv4 address designed for dynamic cloud computing. An Elastic IP address is associated with your AWS account. With an Elastic IP address, you can mask the failure of an instance or software by rapidly remapping the address to another instance in your account.

An Elastic IP address is a public IPv4 address, which is reachable from the internet. If your instance does not have a public IPv4 address, you can associate an Elastic IP address with your instance to enable communication with the internet.

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.