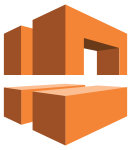
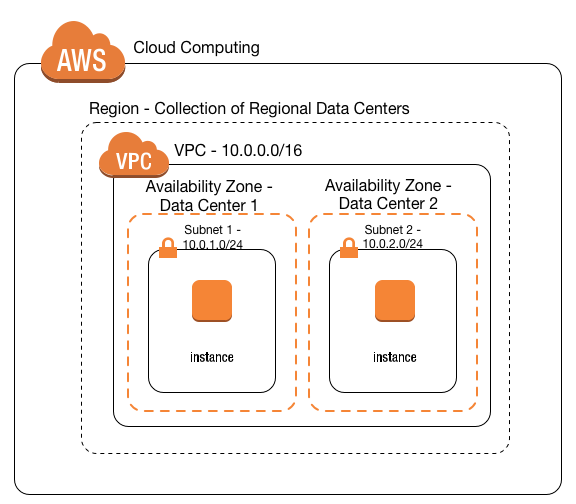
**VPC General**

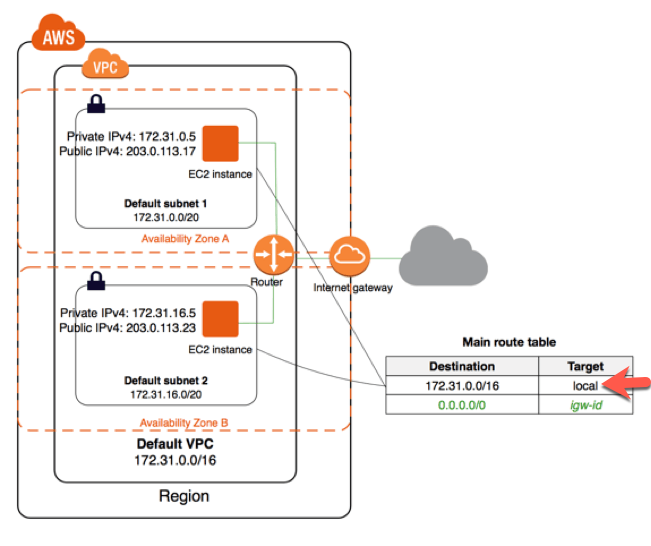


* Amazon **Virtual Private Cloud (VPC)** lets you provision a logically isolated section of the Amazon Web Services (AWS) cloud where you can launch AWS resources in a virtual network that you define.
* Provides complete control over the virtual networking environment including a selection of IP ranges, creation of subnets, and configuration of route tables and gateways.
* A VPC is logically isolated from other VPCs on AWS.
* A default VPC is automatically created for each AWS account the first time Amazon EC2 resources are provisioned.
* VPCs are Region Specific and they do not span regions
* You can create up to 5 VPCs per region
* Every region comes with a default VPC
* You can have 200 subnets per VPC
* You can use IPv4 CIDR block and in addition to IPv6 CIDR blocks (the address of the VPC)
* Cost free: VPC’s, Route Tables, NACL’s, Security Groups, Internet Gateway’s, VPC Peering’s are free of charge
* NAT Gateways, NAT Instance, VPN Gateway, Customer Gateways have cost.
* VPC can assign DNS hostnames to your AWS resources.



**Route Tables**

* The VPC route tables (router) perform routing between AZs within a region.
* The VPC router connects different AZs together and connects the VPC to the Internet Gateway.
* Each subnet has a Route Table. Route tables use to forward traffic within the VPC.
* Route tables also have entries to external destinations.
* Each subnet can only be associated with one route table.
* Can assign one route table to multiple subnets.
* Cannot delete the main route table.



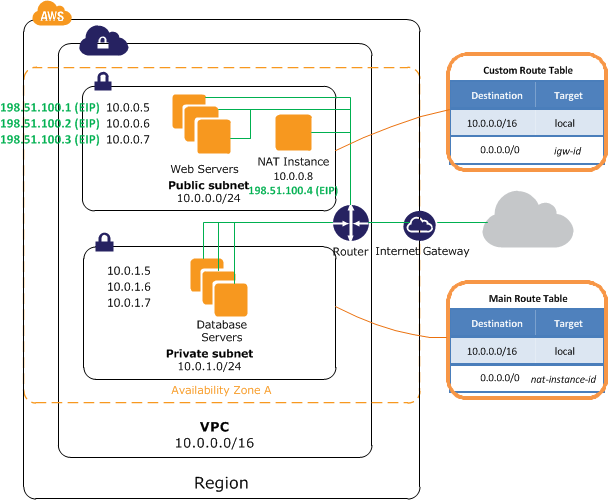
**Subnets**

* Types of subnet:
  + If a subnet’s traffic is routed to an internet gateway, the subnet is known as a **public subnet**.
  + If a subnet doesn’t have a route to the internet gateway, the subnet is known as a **private subnet**.
  + If a subnet doesn’t have a route to the internet gateway, but has its traffic routed to a virtual private gateway for a VPN connection, the subnet is known as a **VPN-only subnet**.
* You cannot create additional CIDR blocks that overlap with existing CIDR blocks.
* 5 IP addresses are reserved by AWS in every subnet. These are the first 4 and last 1 IP address on their CIDR block. 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.
* Internet Gateways (IGW) must be created and then attached to a VPC, be added to a route table, and then associated with the relevant subnet(s).
* If your subnet is associated with a route to the Internet, then it is a public subnet.
* Can only attach 1 IGW to a VPC at a time.
* We can mention 4 different kinds of Gateways
  + **Internet gateway (IGW)** – AWS VPC side of the connection to the public Internet.
  + **Virtual private gateway (VPG)** – VPC endpoint on the AWS side.
  + **Customer Gateway (CGW)** – representation of the customer end of the connection.
  + **Egress-only Internet Gateway** Provides outbound Internet access for IPv6 addressed instances.

**NAT Instance & NAT Gateway**

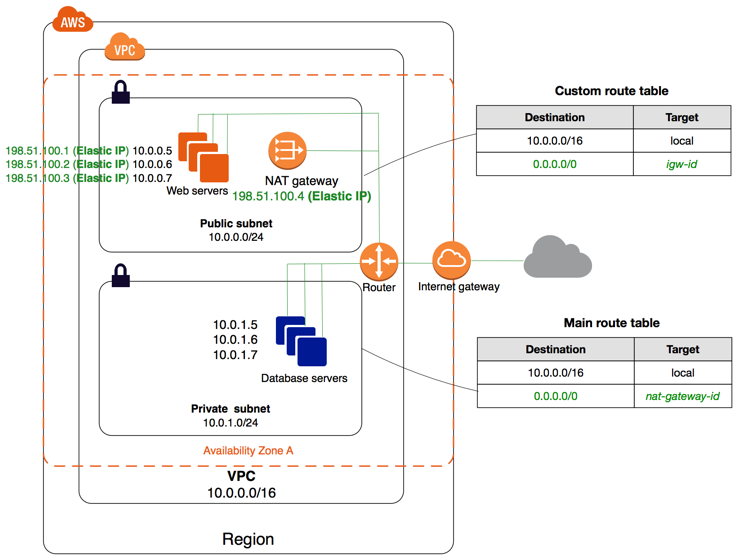
**NAT Instance:**

* NAT Instance is managed by the owner of the account.
* When creating a NAT instance you must **disable source and destination check** on the instance
* NAT instances must exist in a public subnet with a route to an Internet Gateway.
* You must have a route of the private subnet to the NAT instance
* NAT instances need to be assigned to security groups.
* Can use it as a bastion (jump) host.
* The size of a NAT instance determines how much traffic can be handled
* High availability(HA) can be achieved using Autoscaling Groups, multiple subnets in different AZs, and automate failover between them using a script



**NAT Gateway:**

* NAT gateways are fully managed by AWS.
* NAT Gateways are redundant inside an Availability Zone (can survive failure of EC2 instance)
* You can only have 1 NAT Gateway inside 1 AZ (cannot span AZs)
* Starts at 5 GBPS and scales all the way up to 45 Gbps
* Uses an Elastic IP address for the public IP.
* NAT Gateways are the preferred setup for enterprise systems.
* There is no requirement to patch NAT Gateways, and there is no need to disable Source/Destination checks fort he NAT Gateway (unlike NAT instances)
* NAT Gateways are automatically assigned a public IP address.
* Not associated with any security groups.
* Route Tables for the NAT Gateway MUST be uploaded.
* Resource in multiple AZs sharing a Gateway will lose internet access if the Gateway goes down unless you create a Gateway in each AZ and configure route tables accordingly.



**Security Group & Network Access List (NACL)**

**Security Groups:**

* Security Groups acts as a firewall at the instance level
* Useless allowed specifically, all inbound traffic is blocked by default
* All outbound traffic from the instance is allowed by default
* You can specific for the source to be either an IP range, single IP address, or another security group
* Unlike NACL, you can only assign permit rules in a security group, cannot assign deny rules.
* Security Groups are **STATEFULL** (if traffic is allowed inbound it is also allowed outbound)
* Any changes to a Security Group apply immediately.
* You can use security group names as the source or destination in other security groups.
* We can assign multiple security groups to EC2 instances.
* Security groups can include multiple EC2 instances.
* We can not block any specific IP address. For this purpose, we need Network Access List (NACL) tables of subnets.
* You can have 16 Security Groups associated with an ENI (default is 5)

**Network Access List (NACL):**

* Network ACL’s function at the subnet level.
* With NACLs you can have permit and deny rules.
* Network ACLs contain a numbered list of rules that are evaluated in order from the lowest number until the explicit deny.
* Network ACLs have separate inbound and outbound rules and each rule can allow or deny traffic.
* Network ACLs are **STATELESS** so responses are subject to the rules for the direction of traffic.
* NACLs only apply to traffic that is ingress or egress to the subnet not to traffic within the subnet.
* A VPC automatically comes with a default network ACL which allows all inbound/outbound traffic.
* A custom NACL denies all traffic both inbound and outbound by default.
* All subnets must be associated with a network ACL.
* You can create custom NACL’s. By default, each custom network ACL denies all inbound and outbound traffic until you add rules.
* You can associate a network ACL with multiple subnets; however a subnet can only be associated with one network ACL at a time.
* NACLs are the preferred option for blocking specific IPs or ranges.
* Security groups cannot be used to block specific ranges of IPs.
* NACL is the first line of defense, the security group is the second line.
* Changes to NACLs take effect immediately like Security Groups.

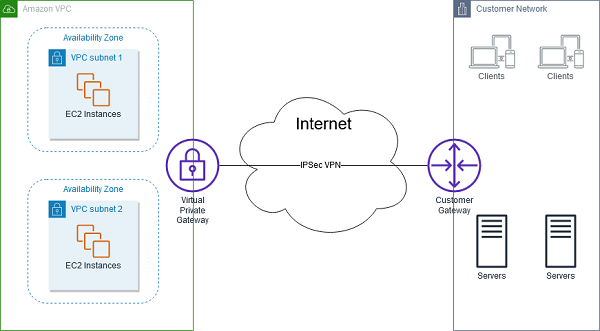
| **Tiobe_Index** |
| --- |

**VPC Connectivity**

* There are several methods of connecting to a VPC. These include:
  + AWS Managed VPN.
  + AWS Direct Connect.
  + AWS Direct Connect plus a VPN.
  + AWS VPN CloudHub.
  + Software VPN.
  + Transit VPC.
  + VPC Peering.
  + AWS PrivateLink.
  + VPC Endpoints.

**AWS Managed VPN:**

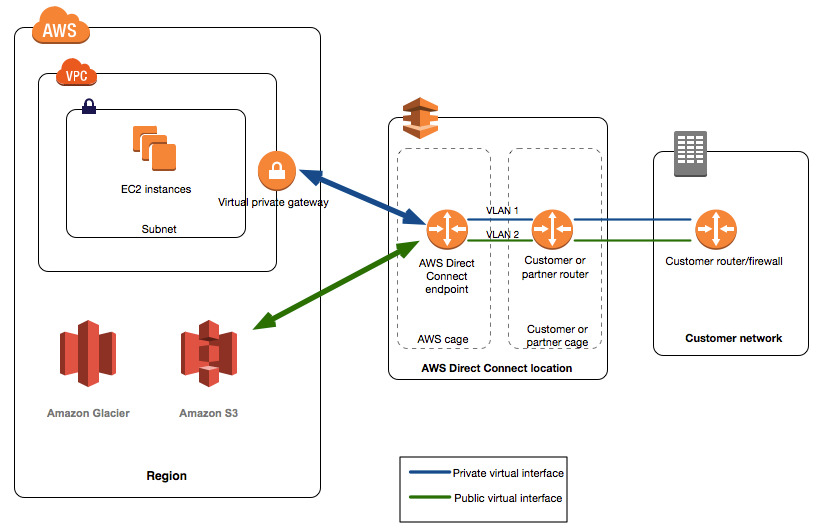
* AWS Managed IPSec VPN connector over your existing internet
* Use case: If you need to establish a secure tunneled connection with a quick and usually simple way to a VPC or redundant link for Direct Connect or other VPN
* A Virtual Private Gateway (VGW) is required on the AWS side
* A customer Gateway is required on the customer side
* An Internet routable IP address is required on the customer gateway.
* Two tunnels per connection must be configured for redundancy.



***AWS Managed VPN***

**AWS Direct Connect:**

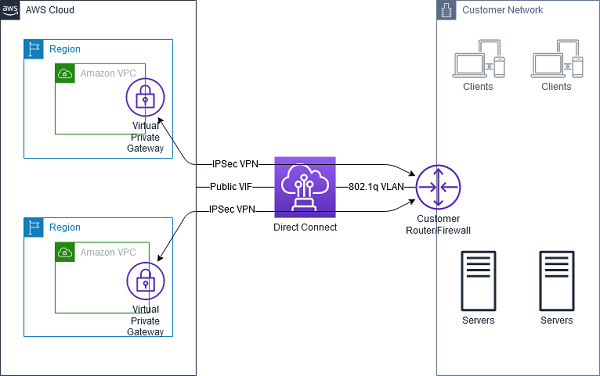
* AWS Direct Connect makes it easy to establish a dedicated connection from an on-premises network to Amazon VPC.
* Using AWS Direct Connect, you can establish private connectivity between AWS and your data center, office, or collocated environment.
* This private connection can reduce network costs, increase bandwidth throughput, and provide a more consistent network experience than internet-based connections.
* AWS Direct Connect lets you establish 1 Gbps or 10 Gbps dedicated network connections (or multiple connections) between AWS networks and one of the AWS Direct Connect locations.
* AWS Direct Connect does not encrypt your traffic that is in transit.
* Use case: When you require a large network link into AWS or lots of resources and services being provided on AWS to your corporate users
* Pros of Direct connect: More predictable network performance; potential bandwidth cost reduction; up to 10 Gbps provisioned connections; supports BGP peering and routing
* Cons of Direct Connection: May require additional telecom and hosting provider relationship and/or network circuits; high cost



**AWS Direct Connect**

**AWS Direct Connect Plus VPN:**

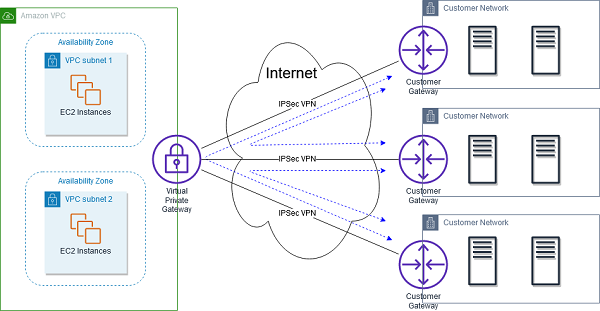
* With AWS Direct Connect plus VPN, you can combine one or more AWS Direct Connect dedicated network connections with the Amazon VPC VPN.
* **Use case:** Need the added security of encrypted tunnels over Direct Connect.
* This solution combines the AWS managed benefits of the VPN solution with low latency, increased bandwidth, more consistent benefits of the AWS Direct Connect solution, and an end-to-end, secure IPsec connection.
* This combination provides an IPsec-encrypted private connection that also reduces network costs, increases bandwidth throughput, and provides a more consistent network experience than internet-based VPN connections.



**AWS Direct Connect plus VPN**

**AWS VPN CloudHub:**

* The AWS VPN CloudHub operates on a simple hub-and-spoke model that you can use with or without a VPC.
* Use case: Link remote offices for back up or primary WAN access to AWS resources and each other -**Use this design** if you have multiple branch offices and existing Internet connections and would like to implement a convenient, potentially low cost hub-and-spoke model for primary or backup connectivity between these remote offices.
* VPN CloudHub is used for hardware-based VPNs and allows you to configure your branch offices to go into a VPC and then connect that to the corporate DC (hub and spoke topology with AWS as the hub).
* Uses a **Border Gateway Protocol (BGP)**.
* Branches can talk to each other (and provides redundancy).
* Can have Direct Connect connections.
* Hourly rates plus data egress charges.



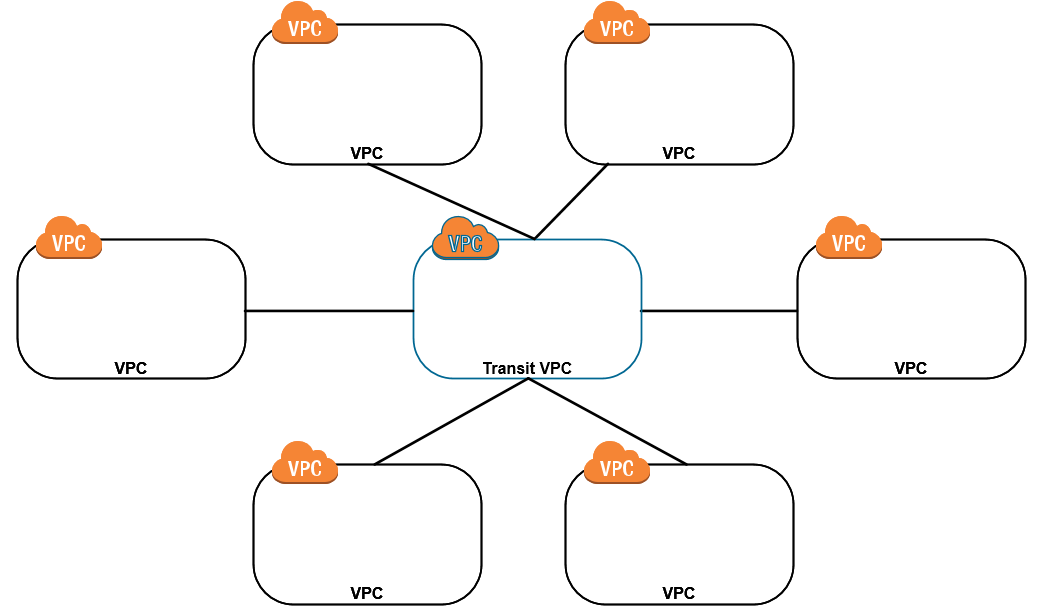
**AWS VPN Cloudhub**

**Software VPN:**

* Amazon VPC offers you the flexibility to fully manage both sides of your Amazon VPC connectivity by creating a VPN connection between your remote network and a software VPN appliance running in your Amazon VPC network.
* **Use case:** You must manage both ends of the VPN connection for compliance reasons or you want to use a VPN option not supported by AWS
* This option is recommended if you must manage both ends of the VPN connection either for compliance purposes or for leveraging gateway devices that are not currently supported by Amazon VPC’s VPN solution.

**Transit VPC:**

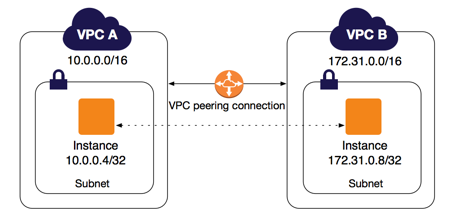
* Building on the Software VPN design mentioned above, you can create a global transit network on AWS. If you need to connect different VPC’s and handle them in one point think transit VPC.
* **Use case:** Locations and VPC-deployed assets across multiple regions that need to communicate with one another
* A transit VPC is a common strategy for connecting multiple, geographically disperse VPCs and remote networks in order to create a global network transit center.
* A transit VPC simplifies network management and minimizes the number of connections required to connect multiple VPCs and remote networks.



**AWS Transit VPC**

**VPC Peering:**

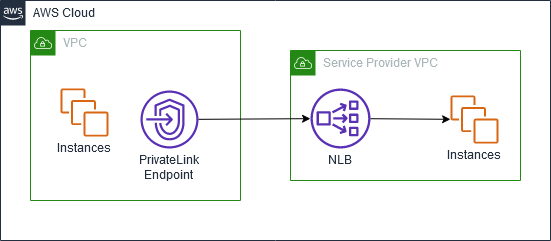
* A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses.
* **Use Case:** Multiple VPS’s need to communicate or access each other’s resources
* Instances in either VPC can communicate with each 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.
* The VPCs can be in different regions (also known as an inter-region VPC peering connection).
* Data sent between VPCs in different regions is encrypted (traffic charges apply)
* Can only have one peering connection between any two VPCs at a time.
* Can peer with other accounts (within or between regions).
* You can create multiple VPC peering connections for each VPC that you own, but transitive peering relationships are not supported.
* Must update route tables to configure routing.
* Need to accept the pending access request in the peered VPC.



**AWS PrivateLink:**

* AWS PrivateLink simplifies the security of data shared with cloud-based applications by eliminating the exposure of data to the public Internet.
* Provides private connectivity between VPCs, AWS services, and on-premises applications, securely on the Amazon network
* Makes it easy to connect services across different accounts and VPCs to significantly simplify the network architecture.
* **Use case:** Keep private subnets truly by using the AWS backbone to reach other AWS or Marketplace services rather than the public internet.

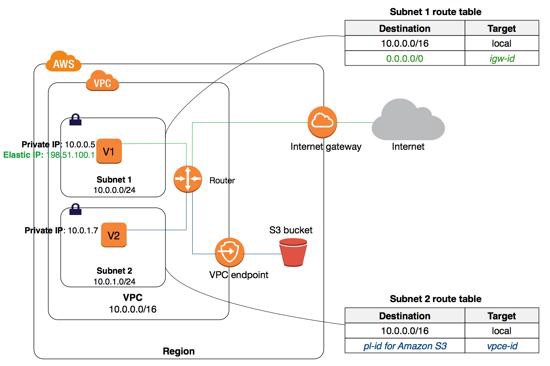
**EXAM TIP:** Know the difference between AWS PrivateLink and ClassicLink. ClassicLink allows you to link EC2-Classic instances to a VPC in your account, within the same region. EC2-Classic is an old platform from before VPCs were introduced and is not available to accounts created after December 2013. However, ClassicLink may come up in exam questions as a possible (incorrect) answer so you need to know what it is.



**AWS Privatelink**

**VPC Endpoints:**

* An Interface endpoint uses AWS PrivateLink and is an elastic network interface (ENI) with a private IP address that serves as an entry point for traffic destined to a supported service.
* Using PrivateLink you can connect your VPC to supported AWS services, services hosted by other AWS accounts (VPC endpoint services), and supported AWS Marketplace partner services.
* An interface VPC endpoint (interface endpoint) enables you to connect to services powered by AWS PrivateLink.
* Gateway endpoints are only available for S3 and DynamoDB
* **Use case:** You can reach S3 and DynamoDB in a private subnet without any internet connection



**AWS VPC Endpoint**

**VPC Flow Logs**

* Flow Logs capture information about the IP traffic going to and from network interfaces in a VPC.
* Flow log data is stored using Amazon CloudWatch Logs.
* VPC Flow Logs can be sent directly to an S3 bucket which allows you to retrieve and analyze these logs yourself.
* You can’t change the configuration of a flow log after it’s been created.