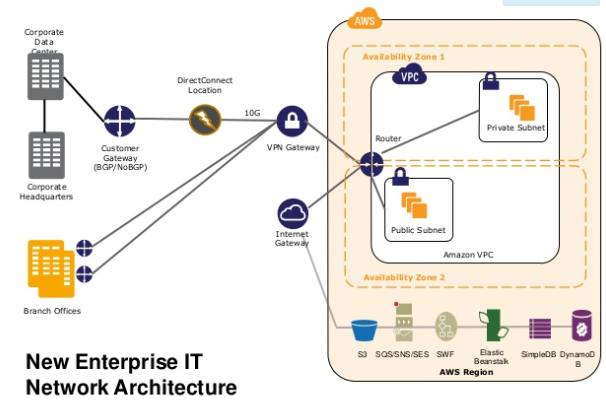
**What is Amazon VPC?**

Amazon Virtual Private Cloud (Amazon VPC) enables you to launch Amazon Web Services (AWS) resources into a virtual network that you've defined.

This virtual network closely resembles a traditional network that you'd operate in your own data centre.



### **VPCs and Subnets**

A **virtual private cloud (VPC)** is a virtual network dedicated to your AWS account. It is logically isolated from other virtual networks in the AWS cloud.

You can launch your AWS resources, such as Amazon EC2 instances, into your VPC. You can configure your VPC; you can select its IP address range, create subnets, and configure route tables.

When you create a VPC, you must specify a range of IPv4 addresses for the VPC in the form of a Classless Inter-Domain Routing (CIDR) block; for example, 10.0.0.0/16.

A **subnet**is a range of IP addresses in your VPC (Sub-network). You can launch AWS resources into a subnet that you select. Use a public subnet for resources that must be connected to the Internet, and a private subnet for resources that won't be connected to the Internet.

### **Subnet Routing**

Each subnet must be associated with a **route table**, which specifies the allowed routes for outbound traffic leaving the subnet.

Every Route Table has default local route below.

| **Destination** | **Target** |
| --- | --- |
| 10.0.0.0/16 | Local |

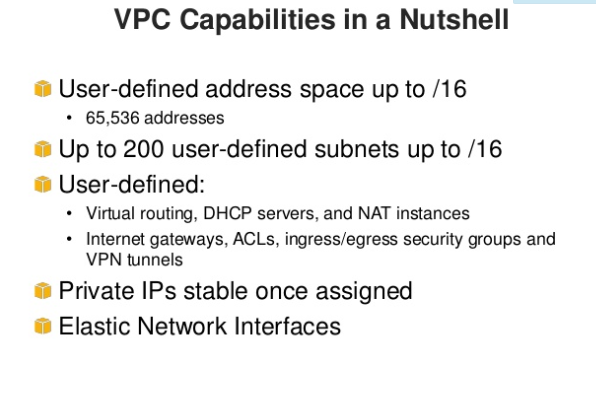
You can easily customize the network configuration of your Amazon VPC. For example, you can create a public-facing subnet for your web servers that have access to the internet. You can also place your backend systems, such as databases or application servers, in a private-facing subnet with no internet access. You can use multiple layers of security, including security groups and network access control lists, to help control access to Amazon EC2 instances in each subnet.

1. To make a Subnet a **public subnet**, we add the route from everywhere to the “Internet gateway” as target, so that in public subnet resources can be accessible from outside/ internet.

| **Destination** | **Target** |
| --- | --- |
| 0.0.0.0/0 | igw-11aa22bb |

1. If we not adding route to Internet gateway in any route table, so every subnet associated with, can be seen as a **Private Subnet**. But to have an internet connectivity for the resources inside private subnet, we add a route target to NAT instance.

| **Destination** | **Target** |
| --- | --- |
| 0.0.0.0/0 | i-342sf522bb |



### **Subnet Security**

AWS provides two features that you can use to increase security in your VPC: **security groups** and **network ACLs**.

Security groups control inbound and outbound traffic for your **instances**, and network ACLs control inbound and outbound traffic for your **subnets**.

Security Group is stateful whereas Network ACL is stateless.

# Internet Gateways

An Internet gateway is VPC component that allows communication between instances in your VPC and the Internet.

Every VPC must be associated with one IGW.

# NAT Instance

# You can use a NAT device to enable instances in a private subnet to connect to the Internet (for example, for software updates) or other AWS services, but prevent the Internet from initiating connections with the instances.

# A NAT device forwards traffic from the instances in the private subnet to the Internet or other AWS services, and then sends the response back to the instances.

We launch the NAT instance in Public Subnet.  
AWS offers two kinds of NAT devices—a NAT gateway or a NAT instance.

A NAT instance is launched from a NAT AMI. Also we need to remember to **Disable Source/destination check**, while launching NAT instance.

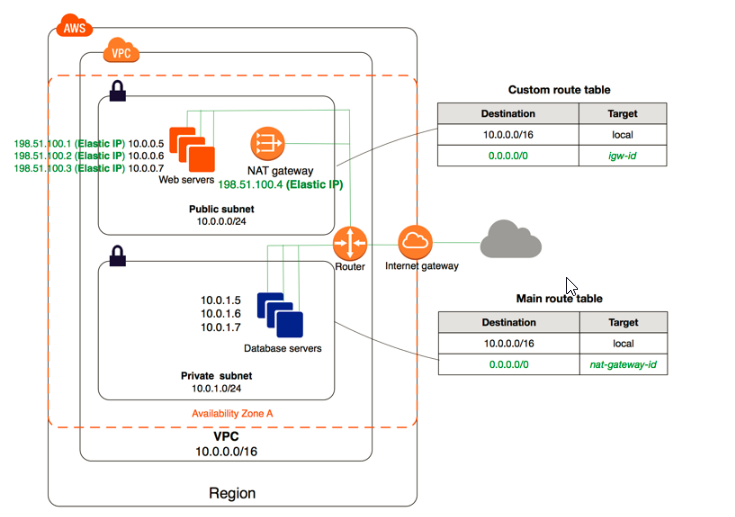
# VPC Peering

A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IP addresses.

Instances in either VPC can communicate with each other as if they are within the same network.

# VPN Connections

# You can connect your VPC to remote networks by using a VPN (Virtual Private Network) connection.



**Questions**

++++++++++++++++++++++++++++++++++++++++++

What is security groups & ACLs? diffrence between them? which one is stateless or statefull n how?

what is VPC? how to define public & private subnets? how to access the internet on public & private subnet?

what is IGW & NAT instance ? how to create NAT instance ? what is routing? ask to define the routes for private & public ?

What is VPC peering?  
  
++++++++++++++++++++++++++++++++++++++++++