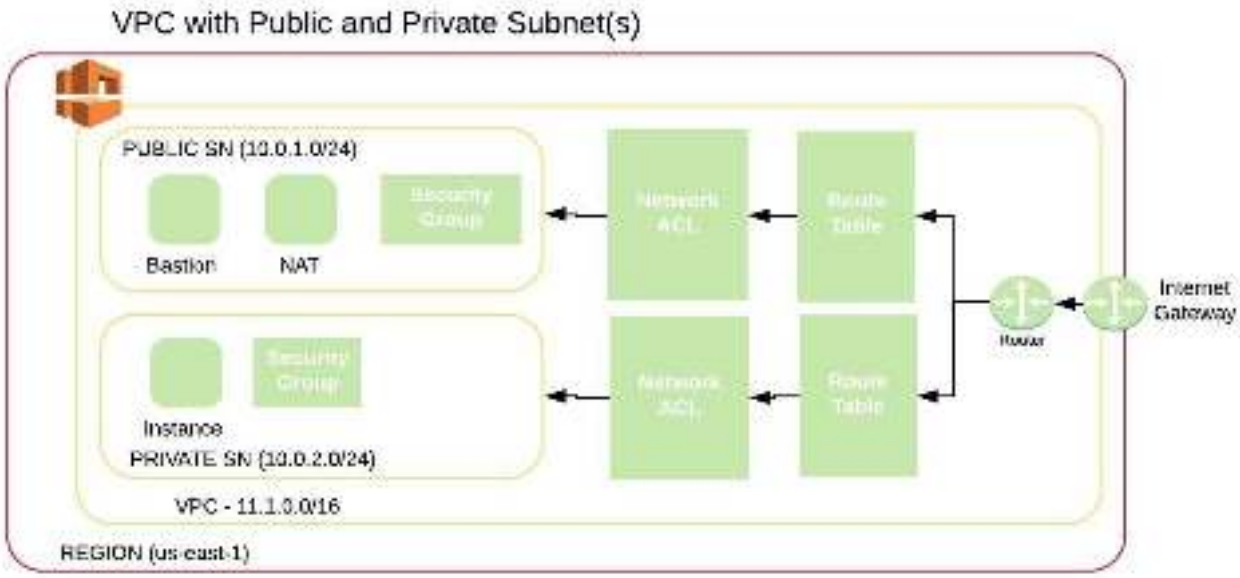
# Virtual Private Cloud (VPC)

VPC is the cornerstone of any cloud deployment. Get an overview of what you can accomplish with a VPC and also take a look at the various peering designs while setting up your cloud deployment.

A VPC is a logically isolated section of a data center where you have complete control over your virtual networking environment, including the selection of IP address ranges, etc.

Think about it like a virtual data center in the cloud.

Additionally, you can create a hardware virtual private Network (VPN) connection between your corporate data center and your VPC and leverage the AWS cloud as an extension of your corporate data center. You can connect into a VPC through an internet gateway or a virtual private gateway.




VPC

Internet Gateway – Router table – Network ACL Public subnet or Private subnet.

Cidr.xyz. Cidr is a notation for describing blocks of IP address and is used heavily in various networking configurations. IP address contains 4 octets

each consisting of 8 bytes giving values between 0 and 255

The decimal value that comes after that; /8 highest address range /12 /16 /28 lowest address range Soft limit 5 VPC by default

**With a VPC you can :-**

1. Launch instances into a subnet
2. Assign custom IP address ranges in each subnet
3. Configure route tables between subnet
4. Create an internet gateway and attach it to your VPC
5. Create Network ACL for better security
6. Instance security groups
7. Subnet network access control links (ACLs)

You can use a Network Address Translation (NAT) gateway to enable instances in a private subnet to connect to the internet or any other service in the cloud. This also protects the VPC from initiating connections with the public internet.

NAT Gateways are a managed service which means that the cloud provider manages this for the customer.

You would have to create a NAT Gateway in each Availability Zone. You should have a route table to route to each NAT Gateway in each availability zone to be able to talk across different AD's.

You would use a network ACL's to control the traffic to and from the subnet in which your NAT gateway resides.

## Network Access Control List (NACL's)

**Review the above diagram.**

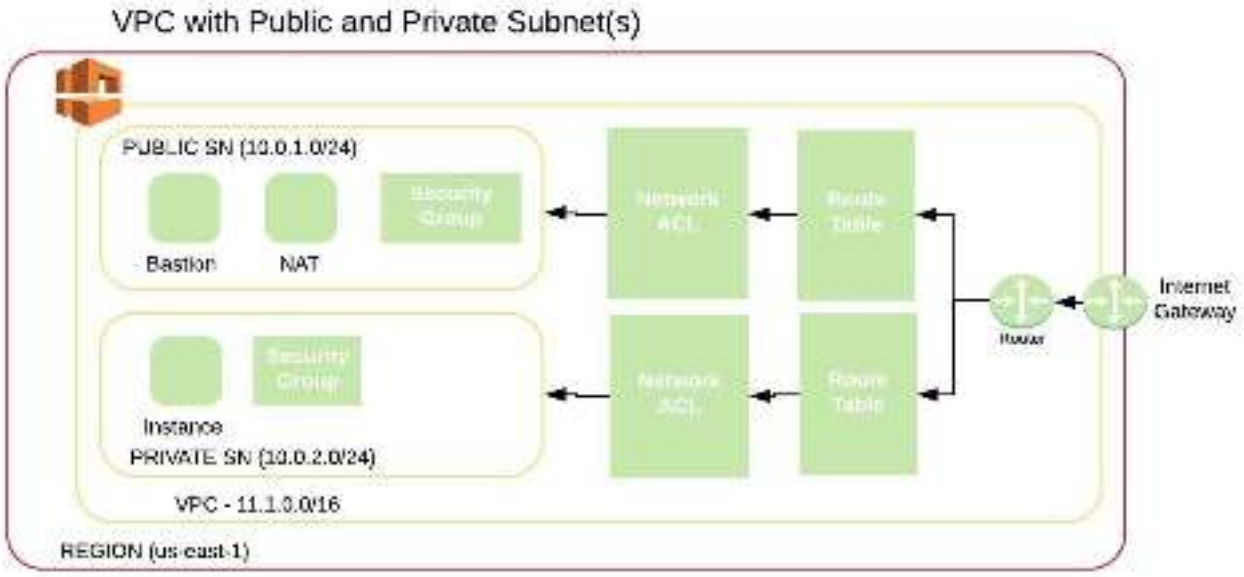
1. We have one instance in a private subnet
2. We have one instance in a public subnet
3. We have a NAT Gateway
4. We have 2 different security groups; one in each subnet.

The network ACL is allowing all the traffic in and out by default

The network ACL is allowing all the traffic in and out by default.

**General Guidance**: you normally can associate one subnet with one NACL, you cannot associate one subnet to multiple NACLs.

However, a network ACL can be associated with multiple subnets.




## NACL

When a user creates a NACL it automatically devices all inbound and outbound until the user adds the rules.

1. Each subnet in your VPC must be associated to a network ACL.
2. Every VPC automatically comes with a default network ACL which by default allows all outbound and inbound traffic.
3. A network ACL contains a numbered list of rules that is evaluated in order, starting with the lowest numbered rule.
4. Network ACL's are stateless which means response to allowed inbound traffic are subject to the rules for outbound traffic and vice versa
5. Network ACL's have separate inbound and outbound rules each rule can either allow or deny traffic.

**VPC Flow Logs**:

VPC Flow logs is a feature that enables you to capture information about the IP traffic going to and from the network interfere into your VPC.

Flow logs data is stored using Amazon cloud Watch logs.

## Bastion

What is a bastion host, and do I need one?

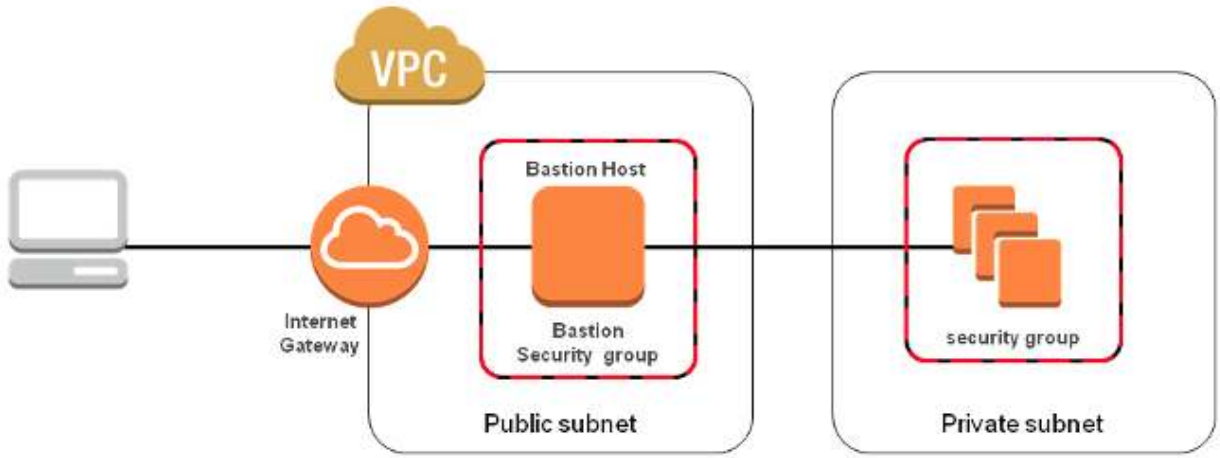
Bastion hosts are instances that sit within your public subnet and are typically accessed using SSH or RDP. Once remote connectivity has been established with the bastion host, it then acts as a 'jump box' server, allowing you to use SSH or RDP to log in to other instances (within private subnets) deeper within your VPC.

When properly configured through the use of security groups and Network ACLs (NACLs), the bastion essentially acts as a bridge to your private instances via the internet.

You may ask yourself, do I need a bastion host in my environment? If you require remote connectivity with your private instances over the public internet, the answer is yes!

This diagram shows connectivity flowing from an end user to resources on a private subnet through a bastion host.

No Image selected




Here are the basic steps for creating a bastion host for your AWS infrastructure:

1. Launch an EC2 instance as you normally would for any other instance.
2. Apply OS hardening as required.

3. Set up the appropriate security groups (SG).
4. Implement either SSH-agent forwarding (Linux connectivity) or Remote Desktop Gateway (Windows connectivity).
5. Deploy an AWS bastion host in each of the Availability Zones you're using.

The NAT instances in the public subnet is used to route the traffic to the instance sitting in the private subnet.

**Jump Boxes / Bastions**

Basically, this allows you to ssh or RDP into Bastion and then initiate a private connection to your instances in the private subnet. The Bastion is hardened and is the only way to administer all the EC2 instances in your private subnet.

## Service Gateway

The service gateway enables an instance in the private sub net to access a public endpoint without actually going through the internet.