DAY- 9

AWS VPC

AWS Architecture and Design

1. Day 1 Overview of Cloud Computing
2. Day 2 Overview of AWS
3. Day 3 Amazon EC2*
4. Day 4 Amazon EBS *
5. Day 5 Amazon CloudWatch *
6. Day 6 Amazon S3*
7. Day 7 Amazon Elastic Load Balancer *
8. Day 8 Amazon Auto Scaling *
9. **Day 9 Amazon VPC ***
10. Day 10 Amazon IAM *
11. Day 11 Amazon RDS
12. Day 12 Amazon Route 53 *
13. Day 13 Amazon DynamoDB* & Glacier
14. Day 14 Amazon Cloudfront* & Import Export & Amazon SES *
15. Day 15 Amazon ElasticBeanStalk & Amazon Cloudformation & Amazon OpsWorks
16. Day 16 AWS Economics & AWS Account Overview *
17. Day 17 AWS Architecture
18. Day 18 AWS Certification Preparation

[With Hands on Demo]

AWS Virtual Private Cloud

AWS VPC

→ What is VPC?

→ Key VPC Terminology

  → Subnets

  → Route Tables

  → Gateways

→ VPC Advanced Features

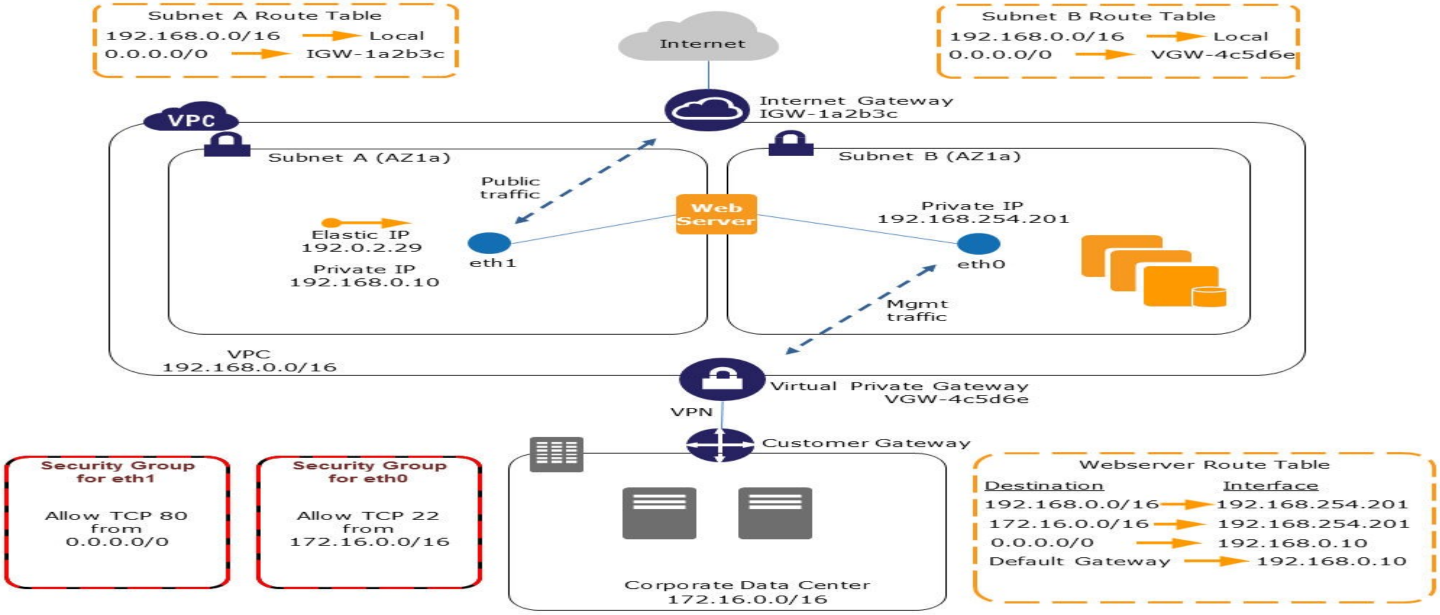
→ Demo

What is Amazon VPC?

Amazon Virtual Private Cloud(Amazon VPC) enables to create a virtual data center in the cloud.

→Define your virtual network

→Logically isolate network for AWS resources



What is Amazon VPC?

- Public & Private Subnets
- Your own IP Address Range with in Subnet
- Simple to use
- Hybrid Cloud
- No Cost
- Added Security Measures

Why VPC?

- Improved Security with Subnets
- Control of Network & IP
- Security Groups & ACL
- Supports new generation of Instance
- Network Isolation for resources
- Fixed IP
- Extend Organization Network
- Direct Connect / VPN
- Supports multiple AWS services
- Multiple IPs to single Instance

Which VPC are You Using?

EC2- Classic

Original EC2

Easy to use but less secure

All instances are publicly accessible and has private and public IP addresses

Security groups allow in-bound rules

Default VPC

Since 4th Dec 2013

Same like Classic-EC2 but with better security

Can use advanced features of VPC when required

VPC

Advanced features of security

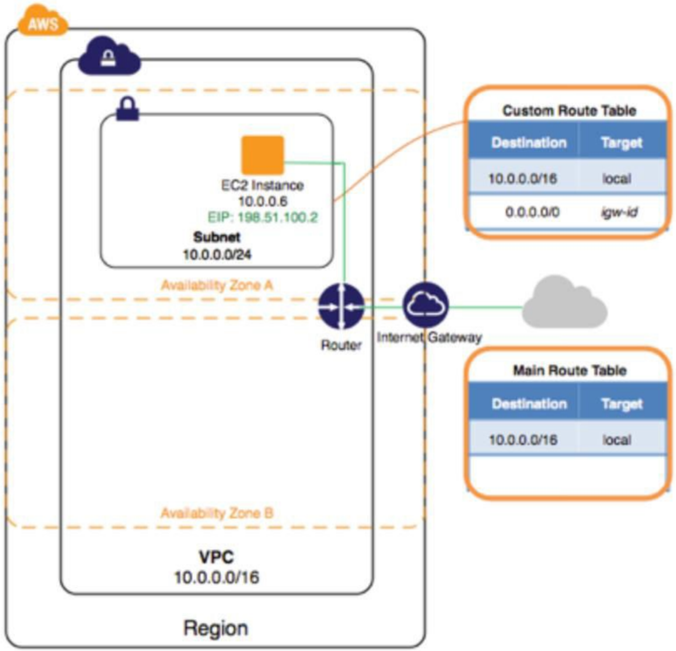
Enhanced networking

Supports ENIs and multiple IPs

Routing tables supports Two-way rules

Subnets, Gateways & Routes

Amazon Virtual Private Cloud 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.



Custom Route Table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	igw-id

Main Route Table

Destination	Target
10.0.0.0/16	local

VPC Fundamentals: Subnets

Range of IP Address

Defined with CIDR Block (10.0.0.0/16)

Public & Private

Public can connect to Internet

Private can connect to public

NAT Instance & NAT Gateway for Private

Belong to only one AZ

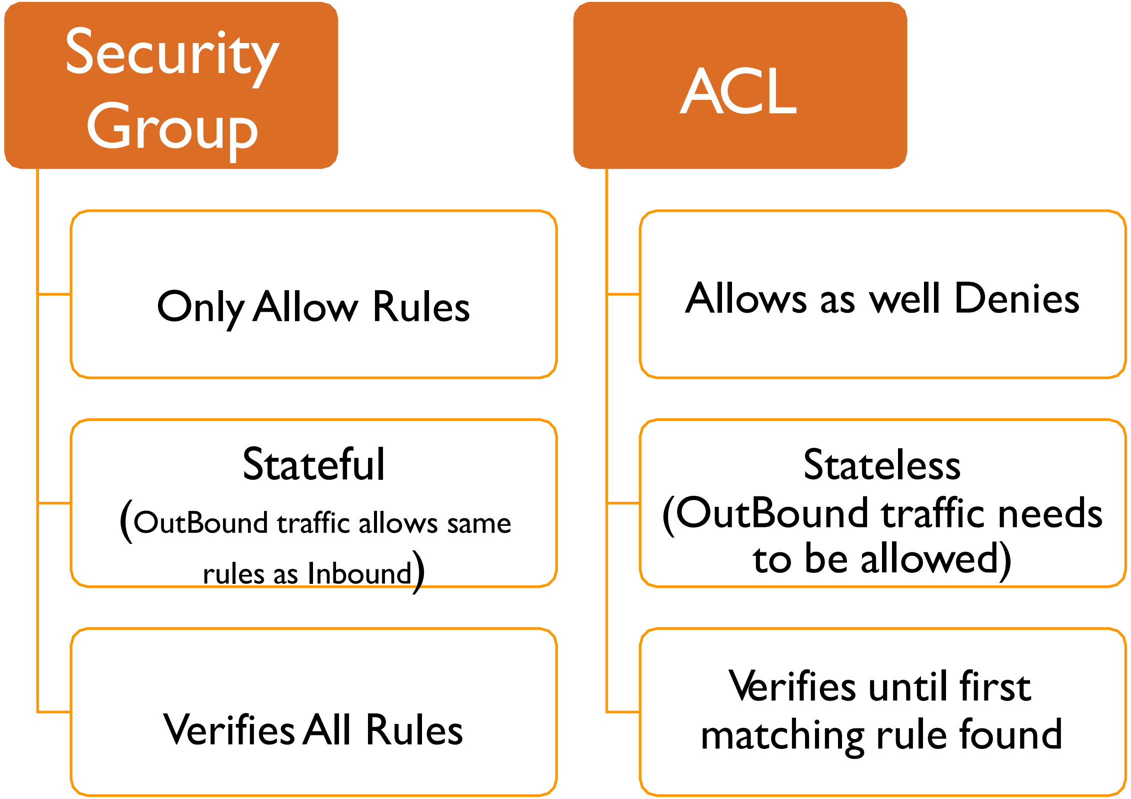
Traffic routed using Route Tables

ACL is Subnet level security

VPC Fundamentals

Security Group	ACL	Route Tables
Firewall for EC2, RDS Instance	Firewall for Subnet	Define IP Routing
Controls Inbound & Outbound Access	Controls Inbound & Outbound Access	Within VPC Each one can communicate

VPC Fundamentals



Security Group

Only Allow Rules

Stateful (OutBound traffic allows same rules as Inbound)

Verifies All Rules

ACL

Allows as well Denies

Stateless (OutBound traffic needs to be allowed)

Verifies until first matching rule found

VPC Fundamentals: Route Tables

Define rules for traffic routing

One subnet one route

Each VPC has minimum one Route Table (main)

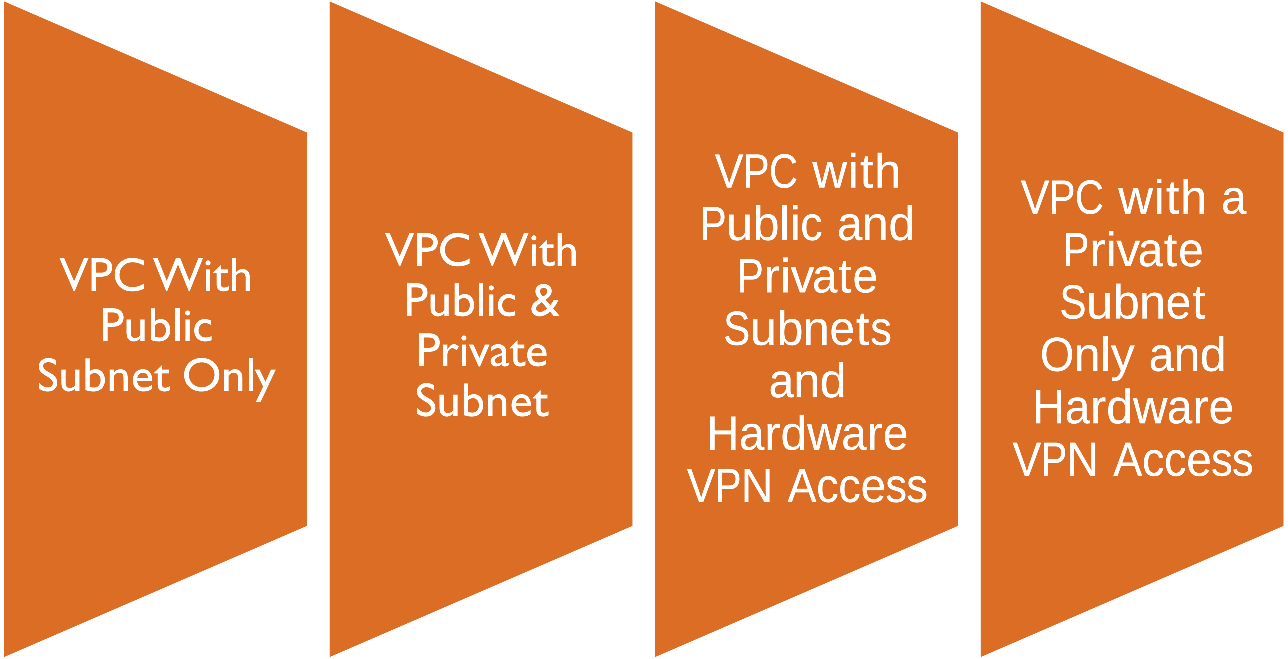
Main Route allows only traffic within VPC

More Route Tables as per need

Separate Route for Public and Private Subnet

VPC Architecture Scenarios

AWS VPC has four architecture scenarios:



VPC With Public Subnet Only

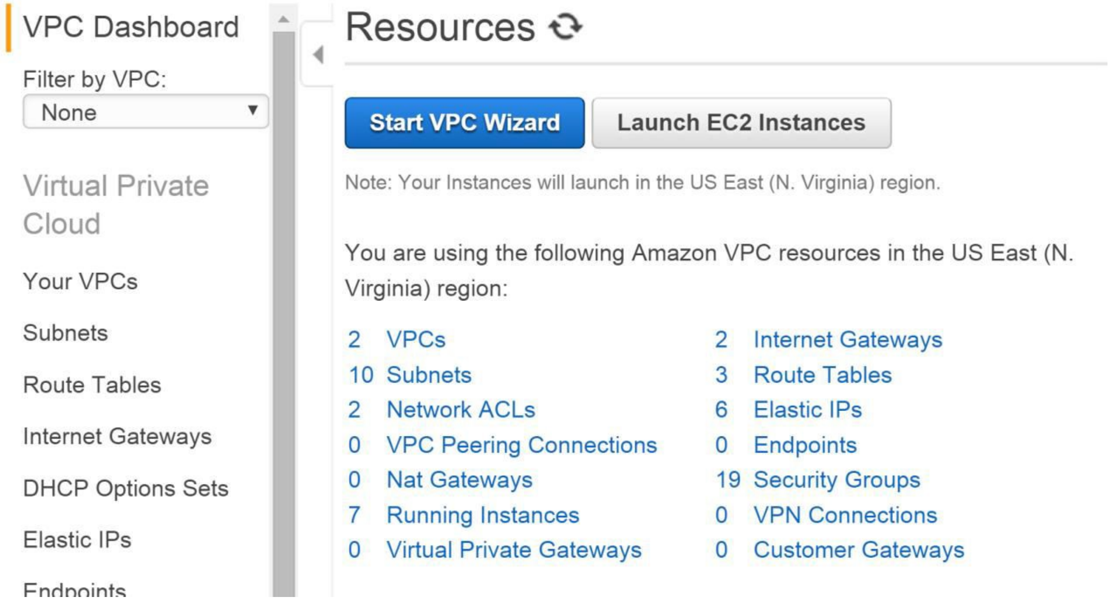
VPC With Public & Private Subnet

VPC with Public and Private Subnets and Hardware VPN Access

VPC with a Private Subnet Only and Hardware VPN Access

Amazon VPC Architecture Scenarios

AWS management console VPC Wizard Start VPC:



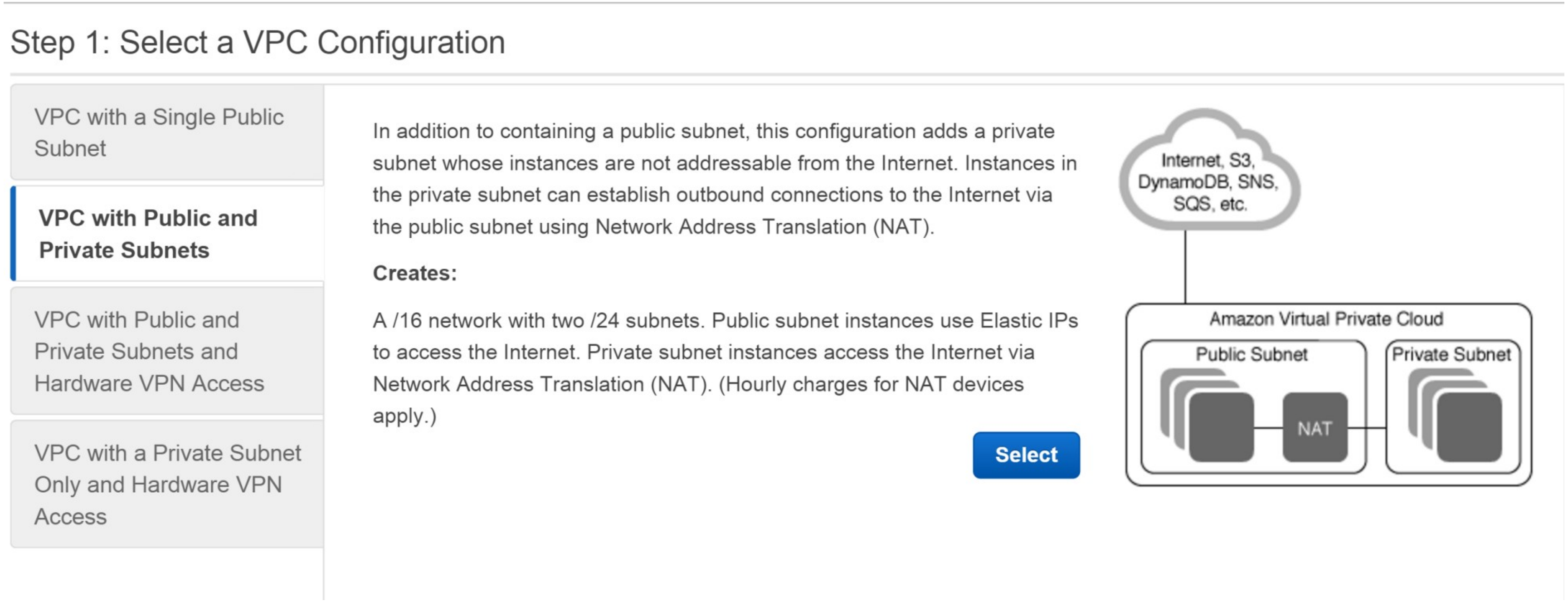
Note: Your Instances will launch in the US East (N. Virginia) region.

You are using the following Amazon VPC resources in the US East (N. Virginia) region:

2	VPCs	2	Internet Gateways
10	Subnets	3	Route Tables
2	Network ACLs	6	Elastic IPs
0	VPC Peering Connections	0	Endpoints
0	Nat Gateways	19	Security Groups
7	Running Instances	0	VPN Connections
0	Virtual Private Gateways	0	Customer Gateways

Amazon VPC Architecture Scenarios

AWS management console VPC Wizard Start VPC Options



Step 1: Select a VPC Configuration

VPC with a Single Public Subnet
VPC with Public and Private Subnets
VPC with Public and Private Subnets and Hardware VPN Access
VPC with a Private Subnet Only and Hardware VPN Access

In addition to containing a public subnet, this configuration adds a private subnet whose instances are not addressable from the Internet. Instances in the private subnet can establish outbound connections to the Internet via the public subnet using Network Address Translation (NAT).

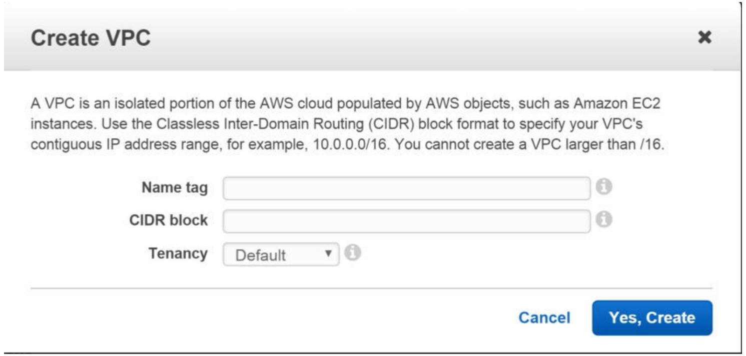
Creates:

A /16 network with two /24 subnets. Public subnet instances use Elastic IPs to access the Internet. Private subnet instances access the Internet via Network Address Translation (NAT). (Hourly charges for NAT devices apply.)

Select
Internet, S3, DynamoDB, SNS, SQS, etc.
Amazon Virtual Private Cloud
Public Subnet
NAT
Private Subnet

Amazon VPC Architecture Scenarios

Create your own VPC manually



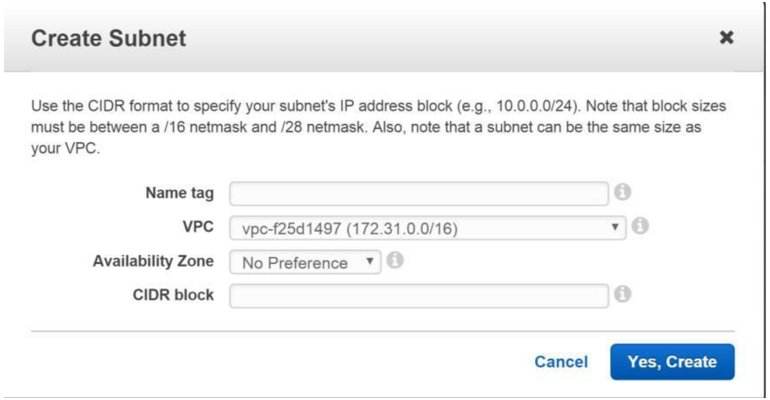
Create VPC

A VPC is an isolated portion of the AWS cloud populated by AWS objects, such as Amazon EC2 instances. Use the Classless Inter-Domain Routing (CIDR) block format to specify your VPC's contiguous IP address range, for example, 10.0.0.0/16. You cannot create a VPC larger than /16.

Name tag

CIDR block

Tenancy: Default



Create Subnet

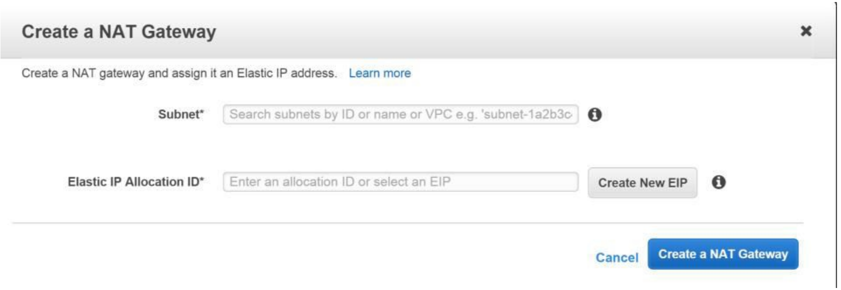
Use the CIDR format to specify your subnet's IP address block (e.g., 10.0.0.0/24). Note that block sizes must be between a /16 netmask and /28 netmask. Also, note that a subnet can be the same size as your VPC.

Name tag

VPC: vpc-f25d1497 (172.31.0.0/16)

Availability Zone: No Preference

CIDR block



Create a NAT Gateway

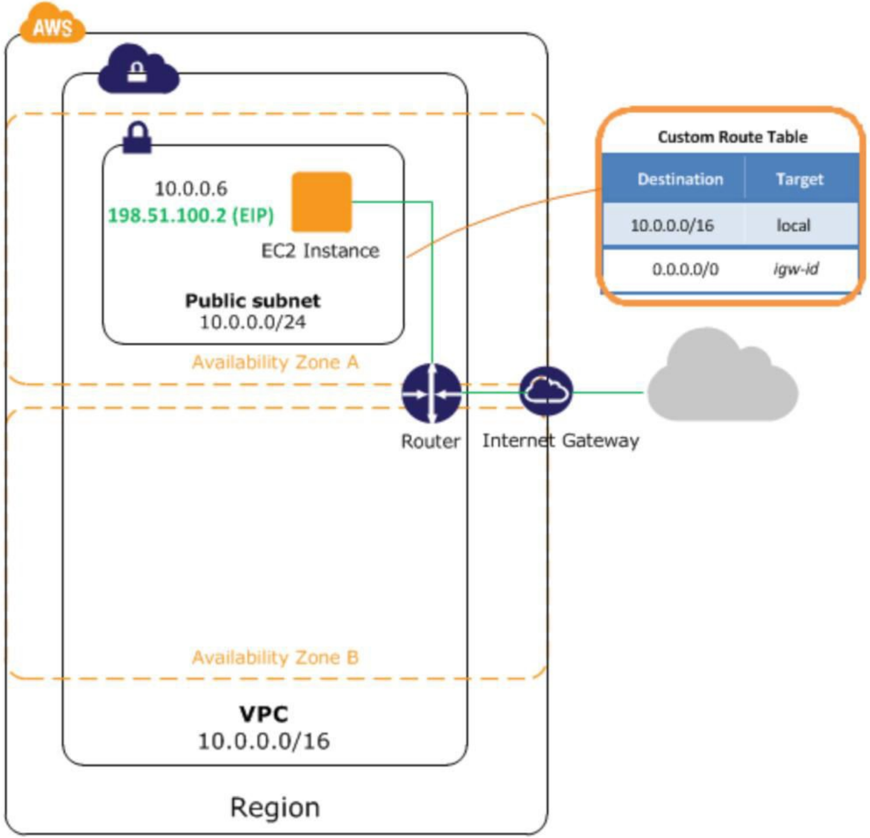
Create a NAT gateway and assign it an Elastic IP address. Learn more

Subnet*: Search subnets by ID or name or VPC e.g. 'subnet-1a2b3c

Elastic IP Allocation ID*: Enter an allocation ID or select an EIP

VPC Architecture Scenarios

1. VPC with a Public Subnet Only



Custom Route Table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	*igw-id*

VPC with a Public Subnet

Access to internet through Internet Gateway

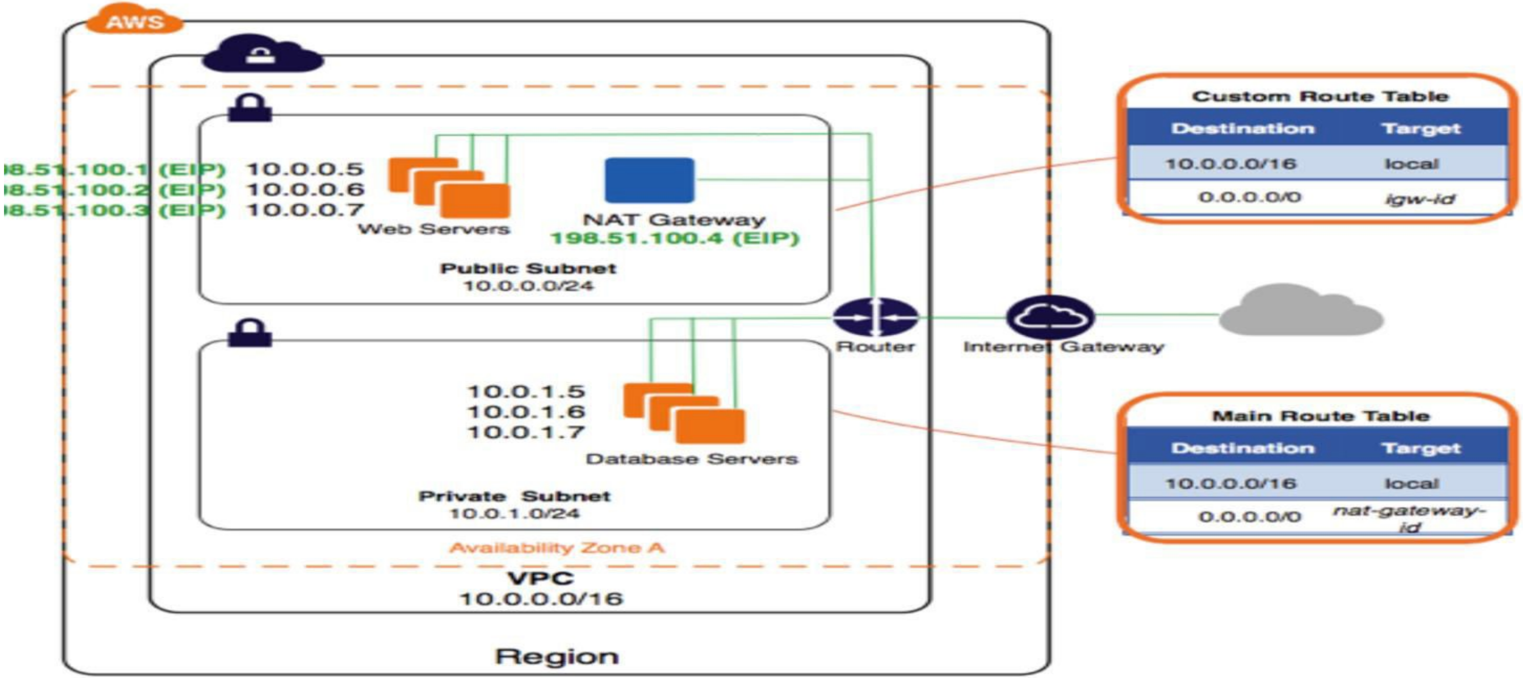
Supports IP range based on CIDR

Each Instance will have public and private IP

Route Table will have entry pointing to Internet Gateway

VPC Architecture Scenarios

2. VPC with Public and Private Subnets



Custom Route Table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	*igw-id*

Main Route Table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	*nat-gateway-id*

VPC with a Public Subnet

Multiple Subnets

Public subnet instance can have Elastic IP

Public subnet connected to Internet Gateway

Private subnet can be reached from public subnet

Private subnet can connect internet with NAT Gateway

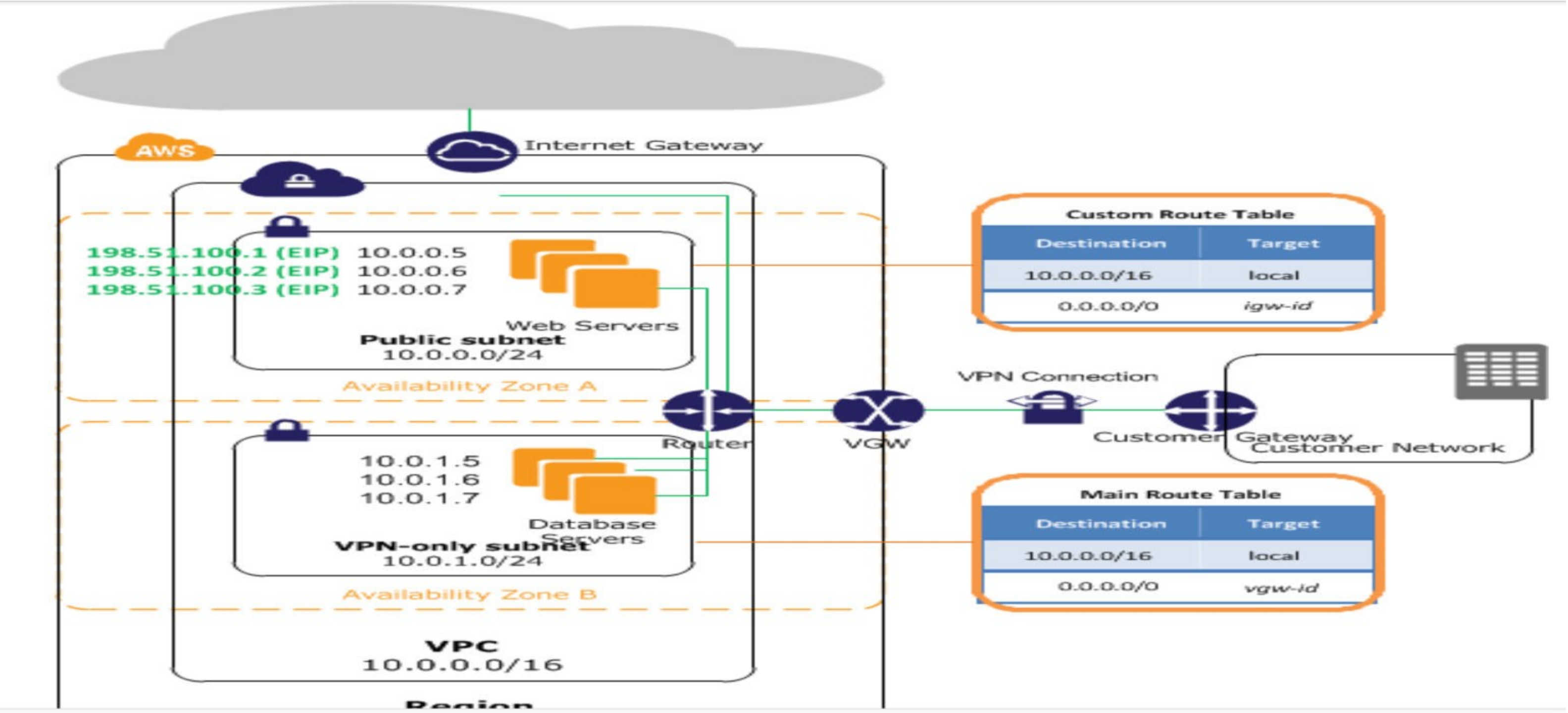
NAT is instance in public subnet with EIP to connect internet

Private subnet for DB / secure data storage

Private subnet route table has entry for routing within VPC as well to NAT

VPC Architecture Scenarios

3. VPC with Public and Private Subnets and Hardware VPN Access



Custom Route Table

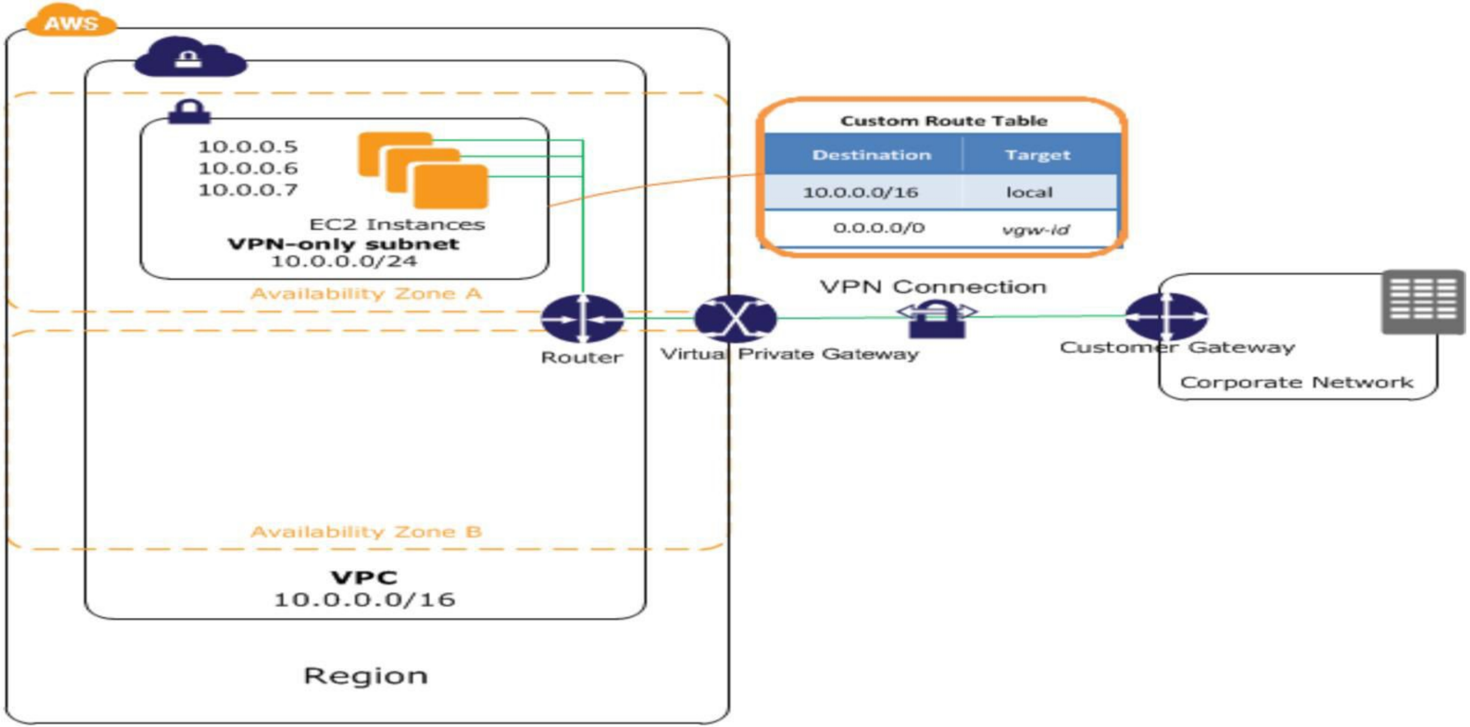
Destination	Target
10.0.0.0/16	local
0.0.0.0/0	igw-id

Main Route Table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	vgw-id

VPC Architecture Scenarios

4. VPC with a Private Subnet Only and Hardware VPN Access



Custom Route Table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	*vgw-id*

Amazon VPC Architecture- Connectivity

Architecture scenarios 3 & 4 were extending an existing on premise corporate network to the Amazon VPC with a VPN

The case 3 &4 are good case for Hybrid Cloud

Amazon VPC Architecture – AWS Products

Products currently available in Amazon VPC are:

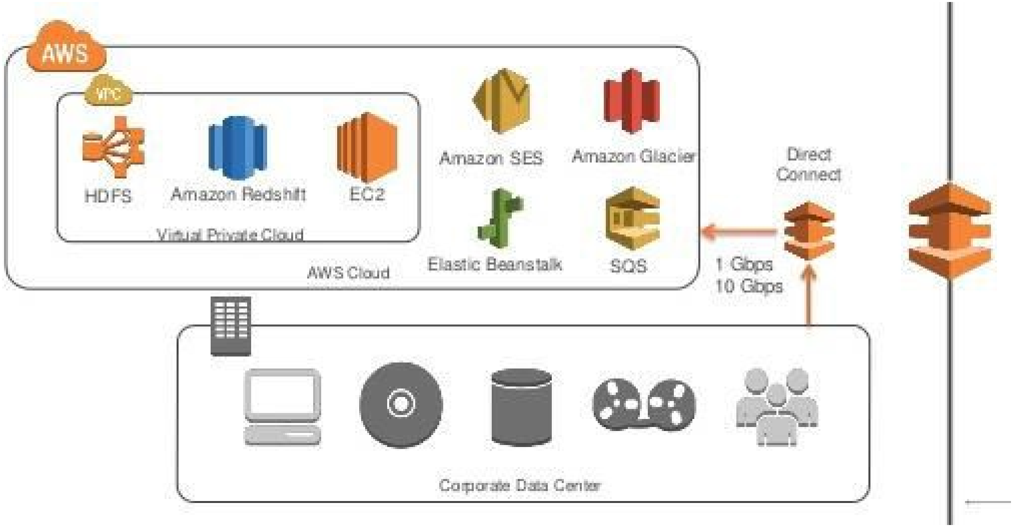
- » Amazon EC2
- » Amazon RDS
- » Auto Scaling
- » Elastic Load Balancing
- » Amazon EMR
- » Elastic Beanstalk
- » ElastiCache
- » Amazon Redshift
- » AWS Data Pipeline

Advanced Features

Amazon VPC includes features such as security groups, network access control lists, VPC Peering and Elastic Network Interfaces(ENIs) as well help in network connectivity.

Amazon VPC Connectivity Options

- Hardware VPN, IPSec hardware VPN Connection.
- AWS Direct Connect, 802.1q VLAN 1Gbps or 10Gbps.
- AWS Direct Connect + VPN, combination of the first two – IPSec VPN and AWS Direct Connect.
- AWS VPN CloudHub, VPN connectivity to multiple customer premises.
- Software VPN, EC2 instance running software VPN, e.g. OpenVPN.



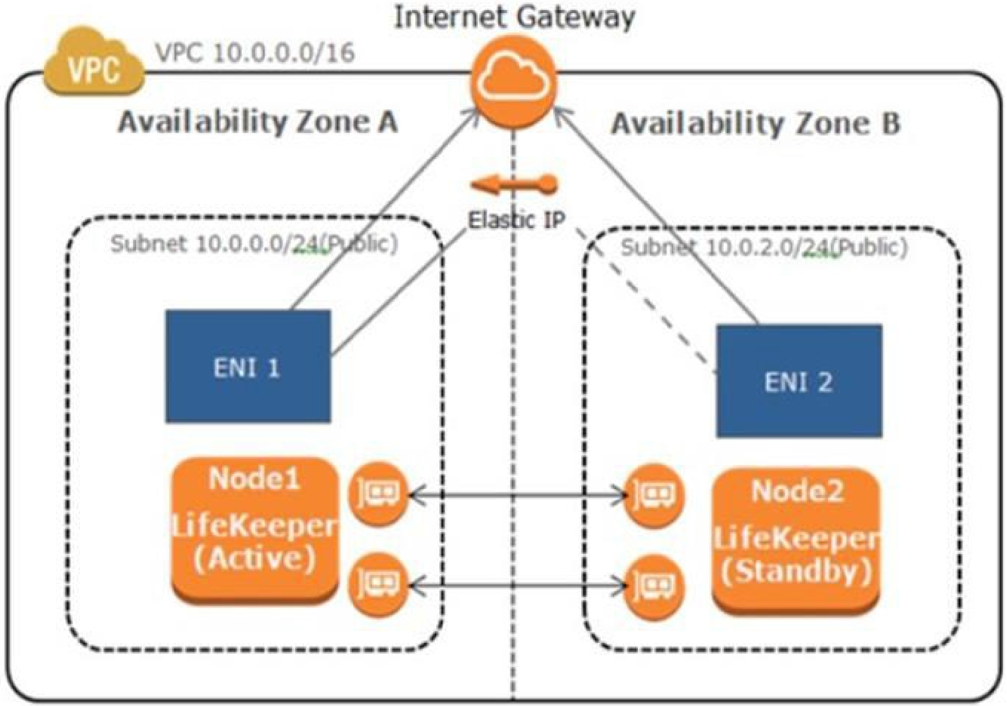
Elastic Network Interface

An elastic network interface is an additional network interface that can be attached to an instance on top of the default network interface

Can attach more than one ENI to one instance

Properties of an ENI:

- » MAC address
- » 1+ private IPS
- » 1 Public EIP(optional)
- » 1+ Security Groups
- » Subnet
- » DeleteOnTermination



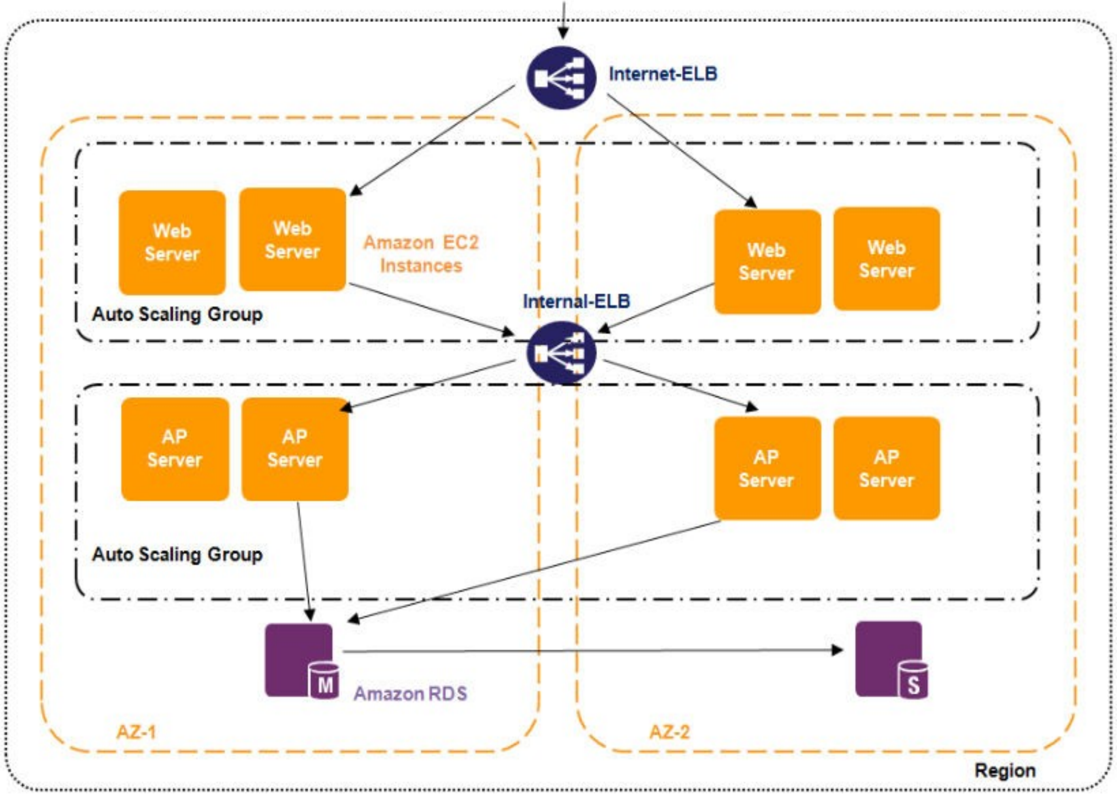
Elastic Load balancing

When you create a load balancer in a VPC, you can make it an internal load balancer or an Internet-facing load balancer.

Load Balancing

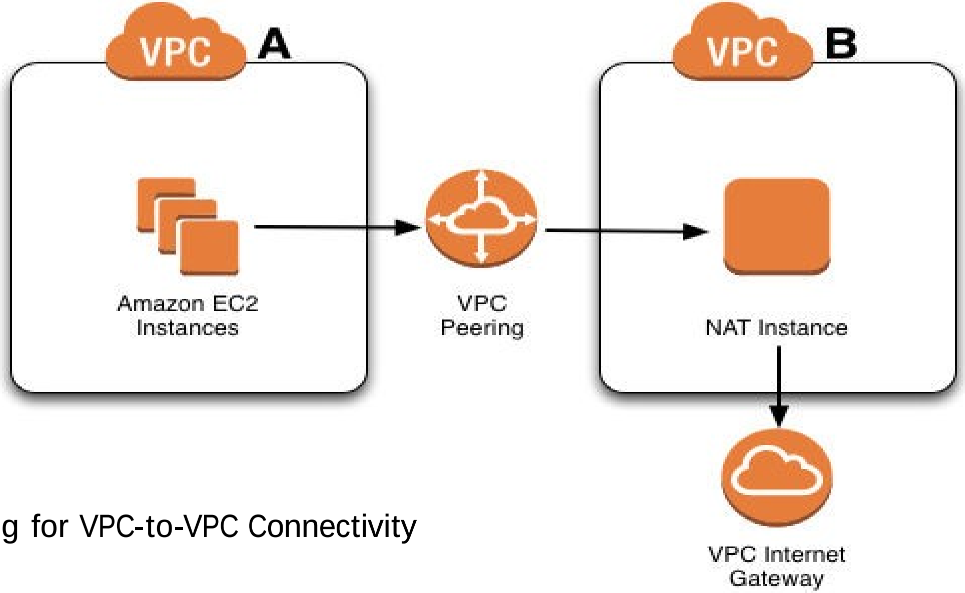
» External ELB

» Mid-tier ELB



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.



VPC peering for VPC-to-VPC Connectivity

Thank You

Email us – support@intellipaat.com

Visit us - https://intellipaat.com