CLOUD COMPUTING

S. Thenmozhi

Department of Computer Applications

CLOUD COMPUTING

Infrastructure as a Service

S.Thenmozhi
Department of Computer Applications

CLOUD COMPUTING

Networking Service

Networking – interconnection of computing devices

VPC – Virtual Private Cloud – which offers the networking service on the cloud

It is a secure, isolated private cloud hosted within a public cloud

VPC combines the scalability and convenience of public cloud computing with data isolation

It is just like reserving a table in a crowded restaurant

Key Technologies used to isolate the a VPC within the public cloud

- Subnet – a range of IP address within the network. In VPC these are private IP addresses which cannot be accessed via public internet
- VLAN – Virtually connecting all the devices without the use of internet
- VPN – uses encryption to create a private network

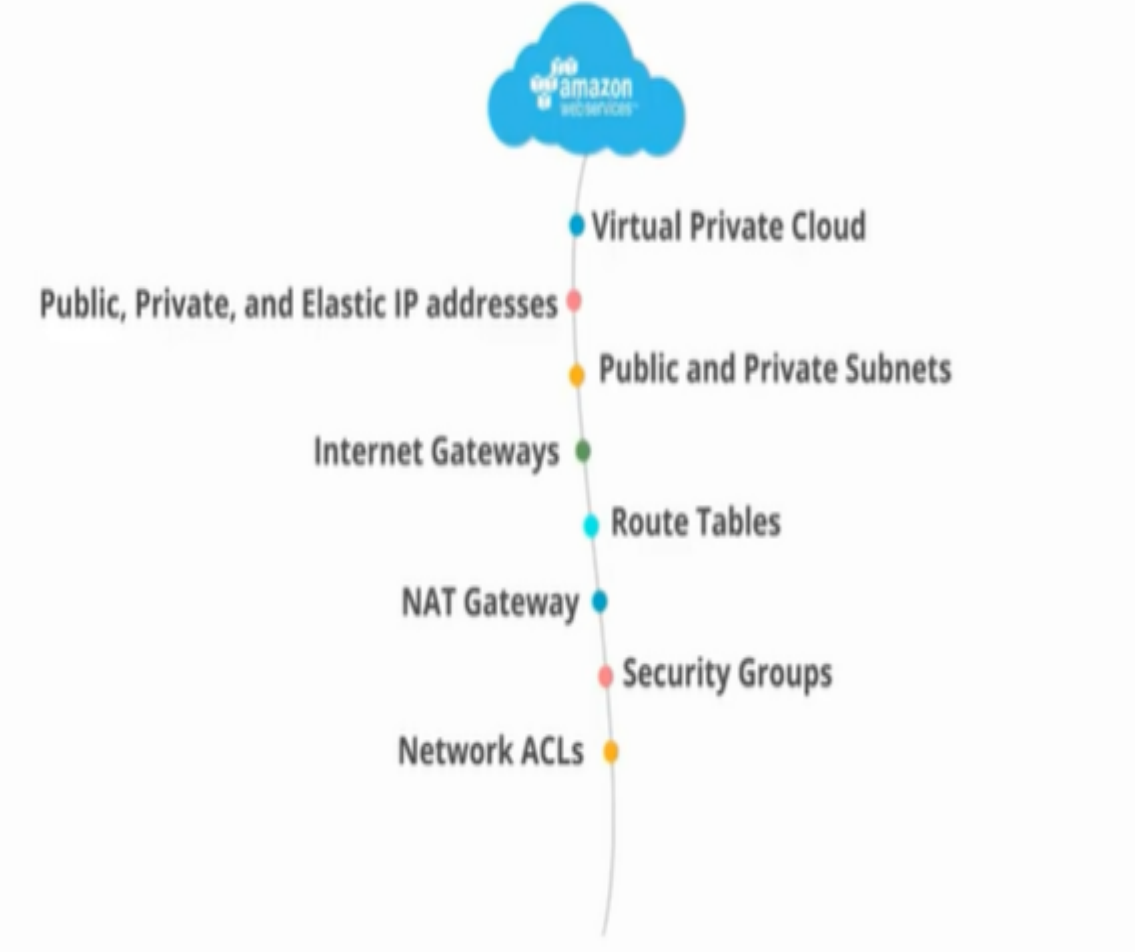
- VPC have the dedicated subnet and VLAN accessible only for VPC customer

Advantages

- Scalability – since VPC is hosted in public cloud, it is easily scalable
- Easy hybrid cloud deployment – on premises infrastructure can be easily connected to VPC through VPN
- Better performance – cloud hosted applications will perform better than hosted on-premises servers
- Better security – taken care by the public CSPs

CLOUD COMPUTING

AWS - VPC

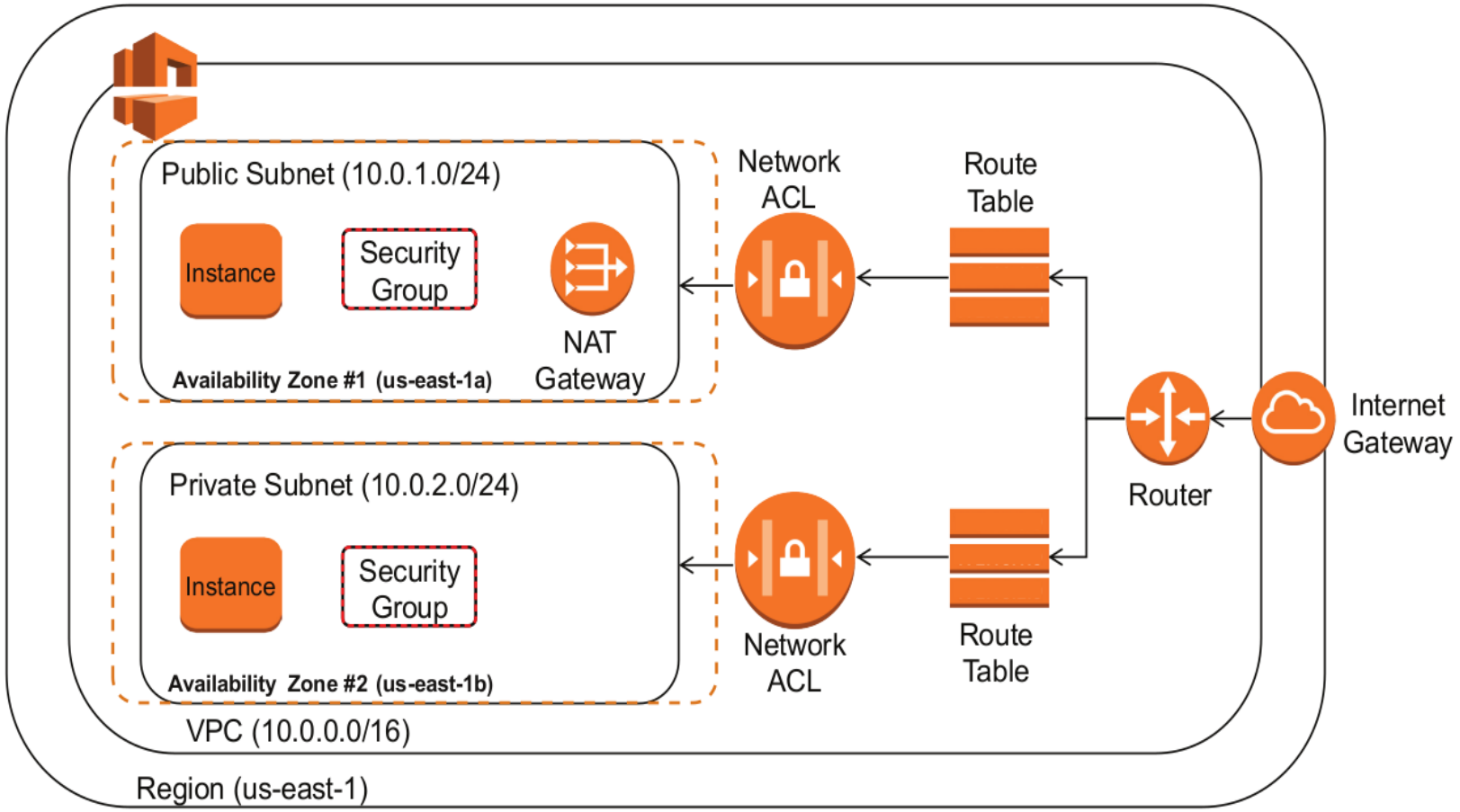


AWS - VPC

- Amazon Virtual Private Cloud (VPC) allows you to create a virtual network within the AWS cloud.
- A VPC is an isolated portion of the AWS cloud in which you can launch Amazon EC2 instances, RDS databases, and other AWS resources.
- VPC allows you to set up an independent network similar to a traditional network operated in an on-premises data-center.

CLOUD COMPUTING

AWS - VPC



Subnet

- A subnet is a range of IP addresses in a VPC in which you can launch Amazon EC2 instances, RDS databases, and other AWS resources.
- A subnet can be public, private, or VPN-only.
  - A **public subnet** is one whose traffic is routed to the Internet using an Internet Gateway.
  - A **private subnet** is one that doesn't have a route to an Internet Gateway. A private subnet is used for resources that are not connected to the Internet.
  - A **VPN-only subnet** is one which has a route to a virtual private gateway and doesn't have a route to an Internet Gateway.

Subnet

- To create a subnet, you must specify your subnet's IP address block in CIDR format,
- Example, 10.0.0.0/24.
- IPv4 block sizes must be between a /16 netmask and /28 netmask and can be the same size as your VPC.

Internet Gateways

- An Internet Gateway (IGW) is a virtual router that connects a VPC to the Internet.
- provides VPC route tables for Internet-routable traffic and performs network address translation (NAT) for instances with public IPv4 addresses.
- During network traffic, IGW translates the destination (public) IP address to the instance's private IP address and forwards the traffic to the VPC.
- For outgoing it does viceversa.

Route Tables

- A route table contains a set of rules which specify how the network traffic is directed.
- Specifies how packets are forwarded between the subnets within your VPC, the Internet, and your VPN connection.
- A subnet in a VPC can be associated with only one route table at a time.
- But, multiple subnets can be associated with the same route table.
- When a VPC is created, it has a main route table which is created automatically.
- You can create additional route tables for a VPC.

NAT Gateways

- A Network Address Translation (NAT) device allows instances in a private subnet connect to the Internet or other AWS services while blocking connections from the Internet to these instances.
- The instances in a private subnet may need a connection to the Internet to download software, updates, and patches.
- AWS provides NAT instances and NAT gateways to allow instances in private subnets connect to the Internet. A NAT instance is setup using an EC2 instance with a NAT Amazon Machine Image (AMI).

Security Groups

- A security group acts like a virtual and stateful firewall for an instance to control inbound and outbound traffic.
- When you launch an instance in a VPC, you can specify the security group.
- If you do not specify a security group, the instance is launched into the default security group which allows inbound traffic from instances assigned to the same security group and allows all outbound traffic.
- In a security group, you can specify allow rules, but not deny rules.

End Points

- A VPC endpoint is a virtual device that allows you to privately connect your VPC
- It can be interface endpoint or gateway endpoint
- Interface endpoint include Amazon EC2 API, SNS, SQS, API Gateway, CloudWatch, and Kinesis Data Streams.
- Gateway endpoint include Amazon S3 and DynamoDB.

THANK YOU

S. Thenmozhi

Department of Computer Applications

thenmozhis@pes.edu

+91 80 6666 3333 Extn 393