BATCH : 149

LESSON : **AWS**

DATE : 25.08.2023

SUBJECT : **VPC-2**

ZOOM GİRİŞLERİNİZİ LÜTFEN **LMS** SİSTEMİ ÜZERİNDEN YAPINIZ

VPC - 2
Elastic IP, Bastion Host, NAT Gateway

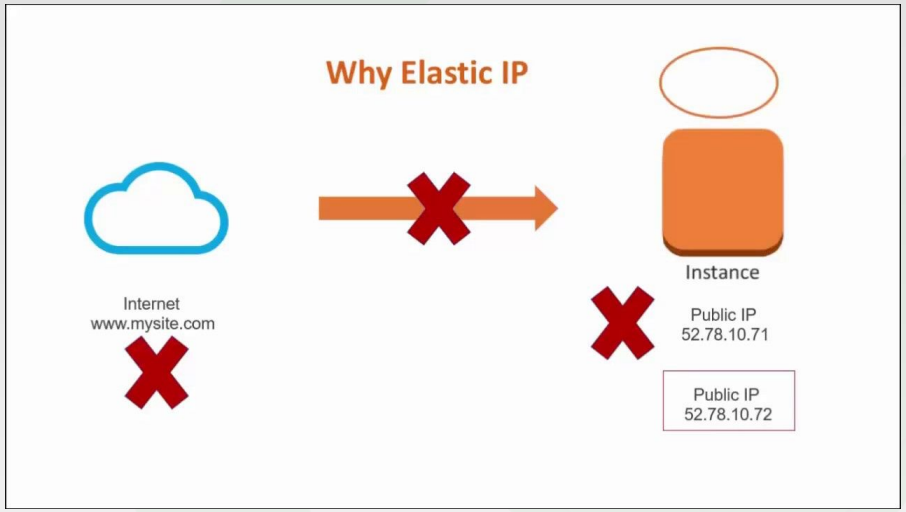
VPC Components

- ✔ **Subnet** — A segment of VPC's IP address range.
- ✔ **Route table** — A set of rules, called routes, that are used to determine where network traffic is directed.
- ✔ **Internet gateway** — A gateway that you attach to your VPC to enable communication between resources in your VPC and the internet.
- ✔ **Egress only Internet Gateway** — Internet Gateway for IPv6
- ✔ **VPC endpoint** — Private connection to public AWS services.
- ✔ **Peering connection** — Direct connection between 2 VPCs.
- ✔ **CIDR block** — Classless Inter-Domain Routing.
- ✔ **Security Group** — Instance level firewall
- ✔ **NACL** — Subnet level firewall

VPC Components

- ✔ **Site-to-Site VPN Connection** — VPN connection between your VPC and on-premises data center or office
  - Uses the Internet
  - **Virtual Private Gateway** — VPC side of a VPN connection
  - **Customer Gateway** — Your side of a VPN connection
  - Encrypted
- ✔ **AWS Direct Connect** — High speed, private network connection from customer to VPC
  - Stable network performance
  - Requires additional line, takes time to set up
  - Not encrypted
- ✔ **Flow Logs** — Capture information about IP traffic inside VPC
  - Logs can be sent to S3 or CloudWatch
- ✔ **Traffic Mirroring** — Allows to capture and inspect network traffic in VPC.
  - You route traffic to security services.
  - Capture packets
  - Used for troubleshooting, content inspection, threat monitoring
- ✔ **Network Firewall** — Layer 3 to Layer 7 managed network firewall and intrusion prevention/detection service that allows customers to filter traffic at the perimeter of their VPC.

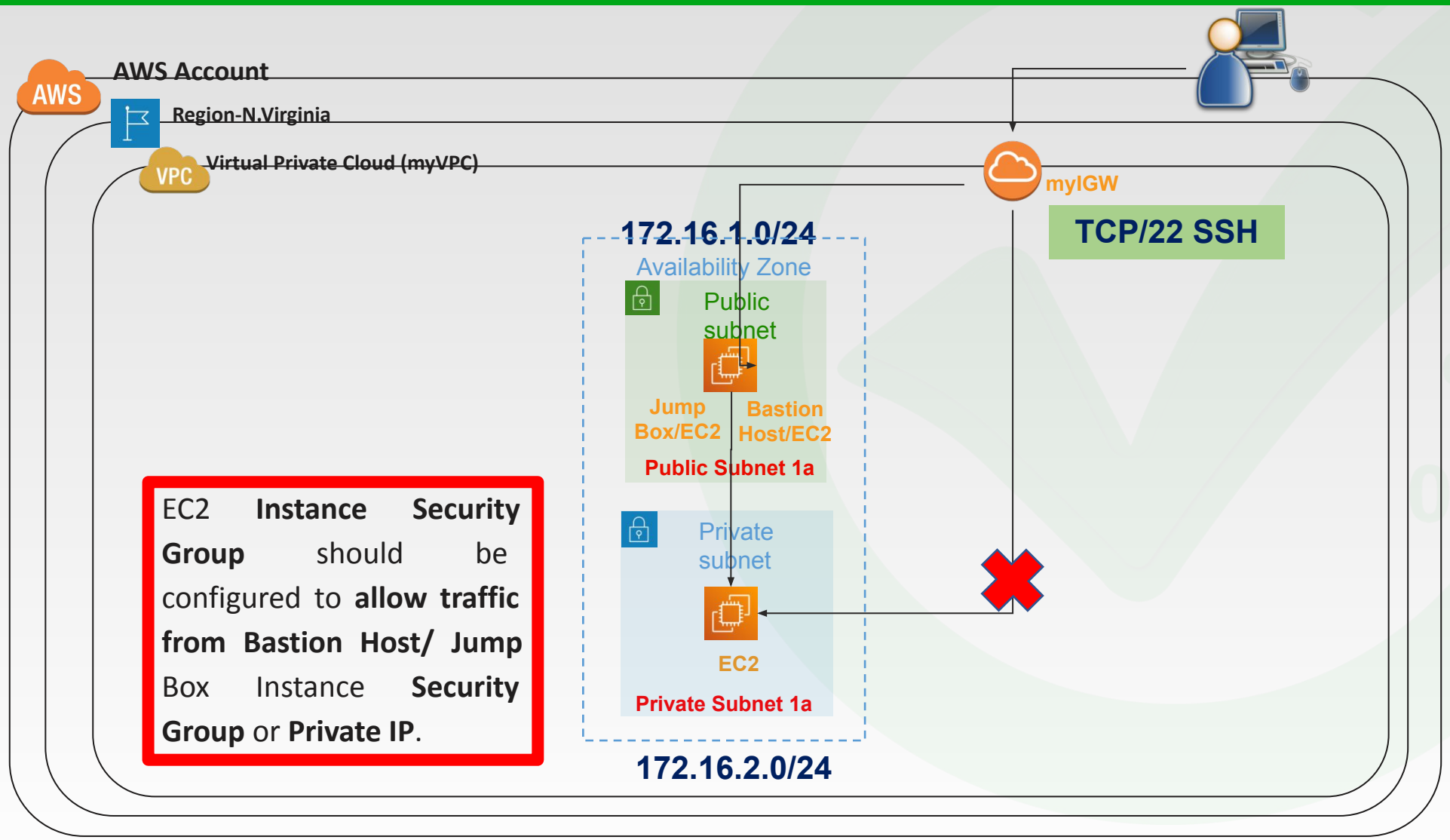
What is Elastic IP?



- ✔ An Elastic IP address is a **Static IPv4 Address.**
- ✔ A **Public IP** address of an instance **is not static and is lost when the instance is stopped,** whereas an **Elastic IP address is a static public address**.
- ✔ Legal requirement for some applications or license policy may render you to use static IP. In addition, some AWS components/services such as **NAT Gateway** and Route53 may need Elastic IP.
- ✔ **Elastic IP is free of charge as long as it is used**. You will be charged for each Elastic IP if you reserve and do not use it.
- ✔ *We currently do not pay for Public IPv4 addresses we use in AWS. However, starting **Feb 2024** AWS **will charge** for them.*

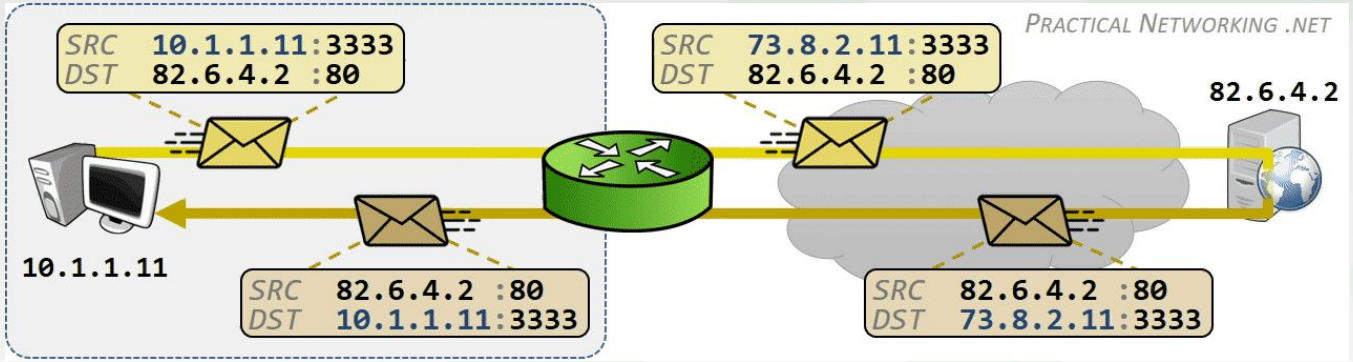
Bastion Host/ Jump Box

Bastion host also known as a **Jump Box** is a particular purpose computer on a network that **acts as a proxy server** and allows the client machines to connect to the remote server. The Bastion hosts are used in cloud environments as a **server to provide access to a private network from an external network such as the Internet**.



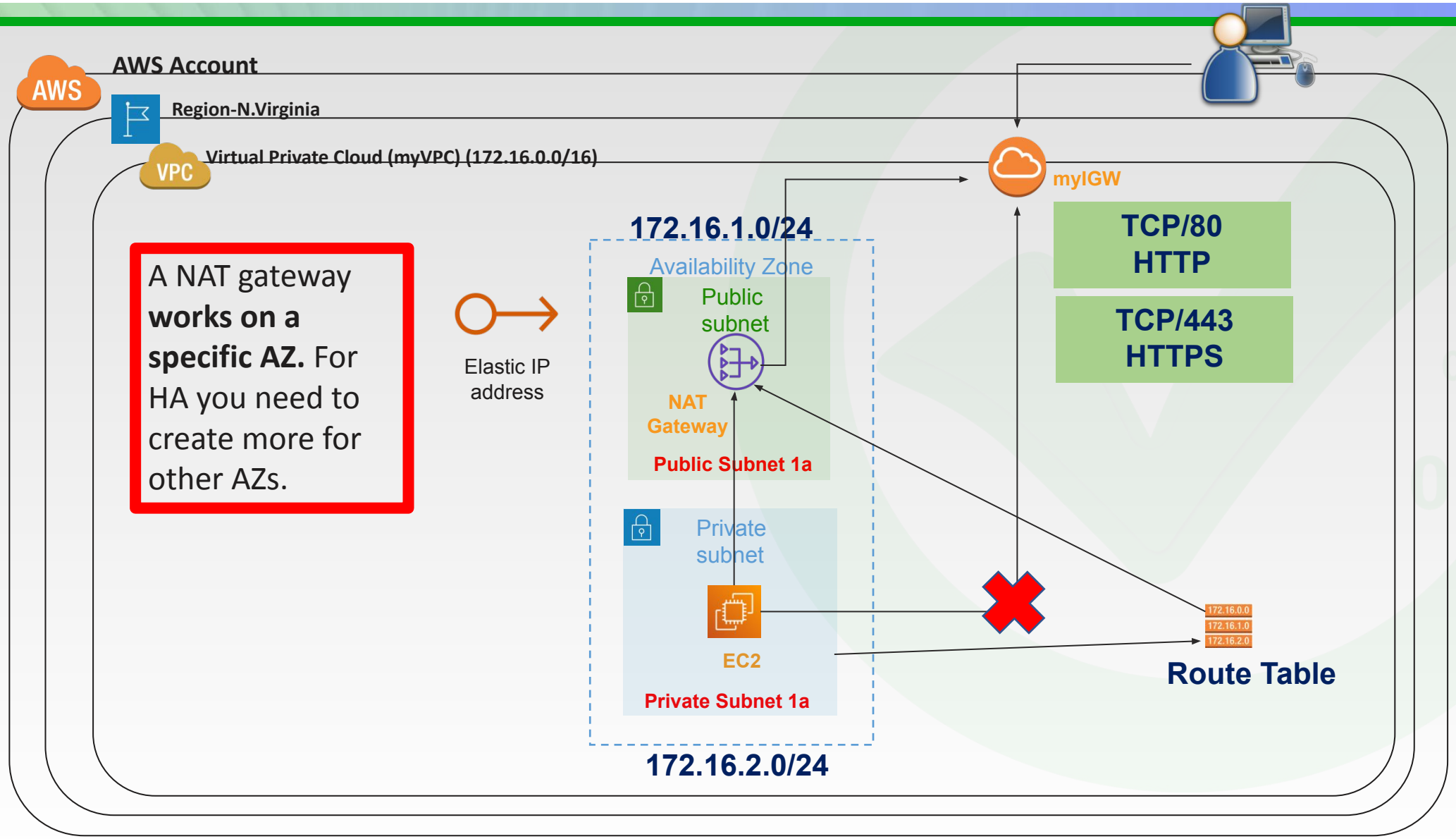
NAT

- NAT stands for network address translation. It's a way to **map multiple private addresses** inside a local network **to a public IP address** before transferring the information onto the internet.
- **Mapping** is done by **changing the header of IP packets** while in transit via a router. This helps to **improve security** and **decrease the number of IP addresses** an **organization needs.**



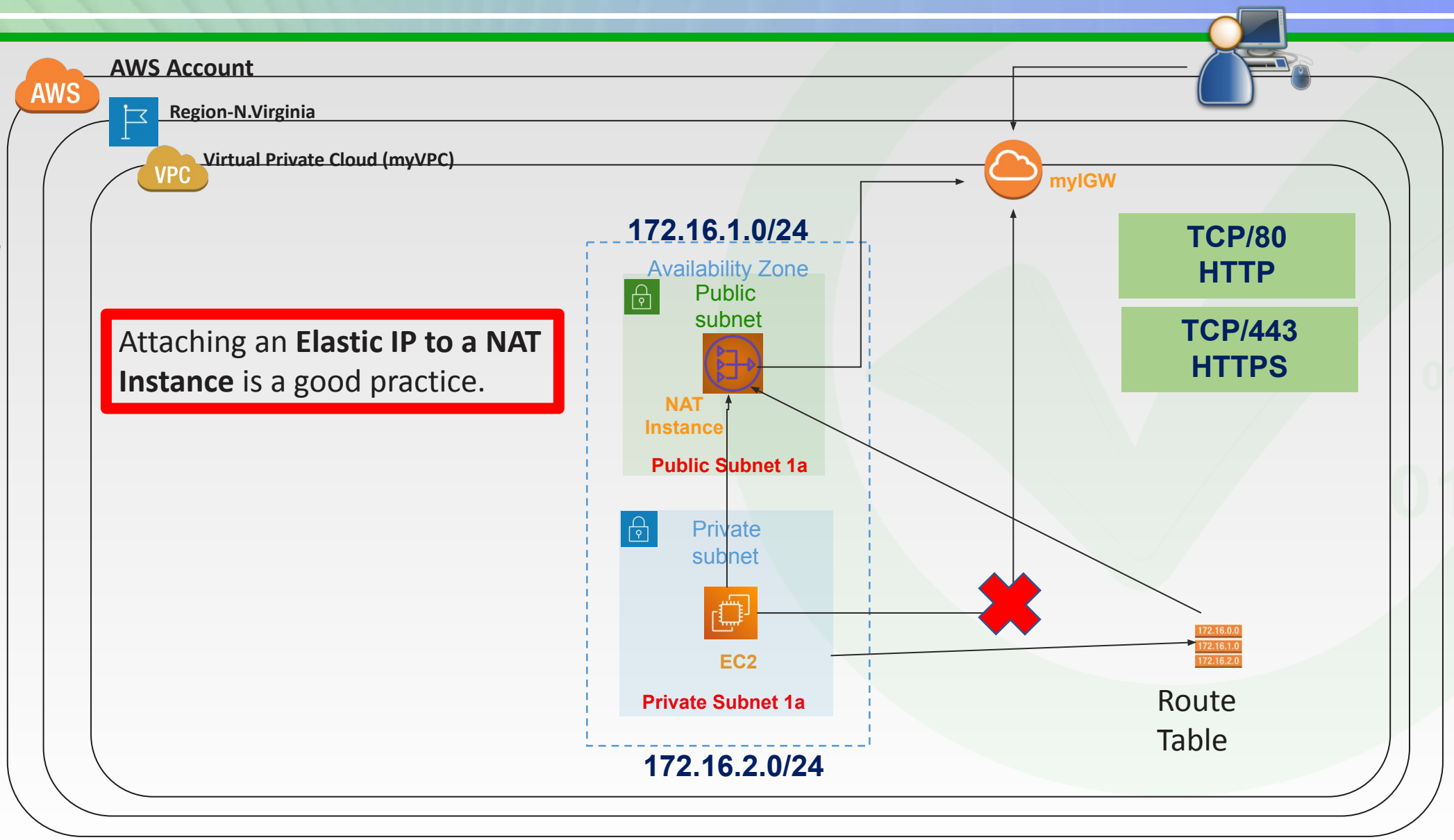
Nat Gateway

A NAT gateway is a Network Address Translation (NAT) service. You can use a NAT gateway so that **instances in a private subnet can connect to services outside your VPC but external services cannot initiate a connection with those instances.**



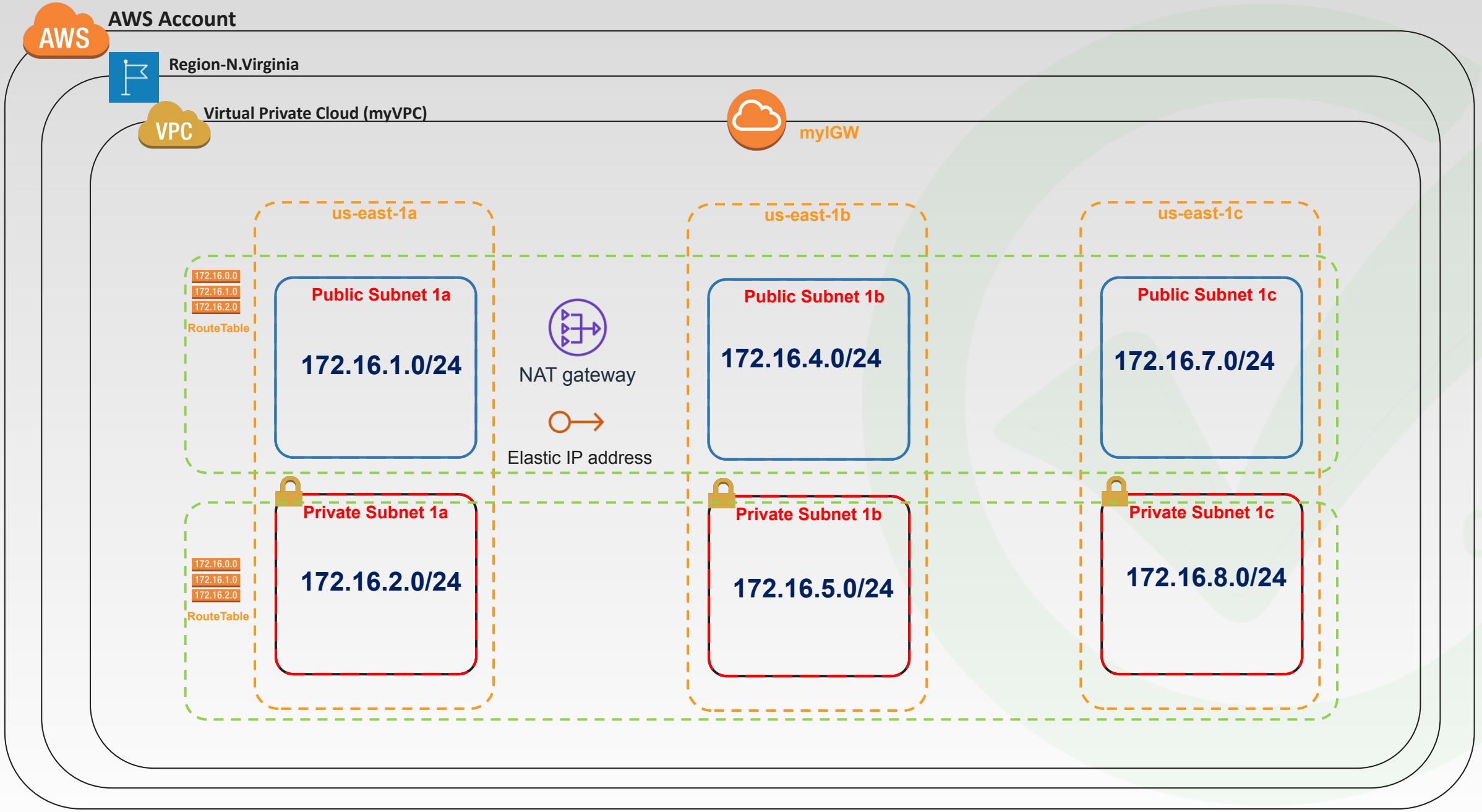
Nat Instance

A **NAT instance behaves like a NAT Gateway. Instances in a private subnet can connect to services outside** your VPC but e**xternal services cannot initiate a connection with those instances.** Source/destination check must be disabled.



Nat Gateway vs Nat Instance

Attribute	NAT gateway	NAT instance
Availability	Highly available. NAT gateways in each Availability Zone are implemented with redundancy. Create a NAT gateway in each Availability Zone to ensure zone-independent architecture.	Use a script to manage failover between instances.
Bandwidth	Scale up to 100 Gbps.	Depends on the bandwidth of the instance type.
Maintenance	Managed by AWS. You do not need to perform any maintenance.	Managed by you, for example, by installing software updates or operating system patches on the instance.
Performance	Software is optimized for handling NAT traffic.	A generic AMI that's configured to perform NAT.
Cost	Charged depending on the number of NAT gateways you use, duration of usage, and amount of data that you send through the NAT gateways.	Charged depending on the number of NAT instances that you use, duration of usage, and instance type and size.
Type and size	Uniform offering; you don't need to decide on the type or size.	Choose a suitable instance type and size, according to your predicted workload.
Public IP addresses	Choose the Elastic IP address to associate with a public NAT gateway at creation.	Use an Elastic IP address or a public IP address with a NAT instance. You can change the public IP address at any time by associating a new Elastic IP address with the instance.
Private IP addresses	Automatically selected from the subnet's IP address range when you create the gateway.	Assign a specific private IP address from the subnet's IP address range when you launch the instance.
Security groups	You cannot associate security groups with NAT gateways. You can associate them with the resources behind the NAT gateway to control inbound and outbound traffic.	Associate with your NAT instance and the resources behind your NAT instance to control inbound and outbound traffic.
Network ACLs	Use a network ACL to control the traffic to and from the subnet in which your NAT gateway resides.	Use a network ACL to control the traffic to and from the subnet in which your NAT instance resides.
Flow logs	Use flow logs to capture the traffic.	Use flow logs to capture the traffic.
Port forwarding	Not supported.	Manually customize the configuration to support port forwarding.
Bastion servers	Not supported.	Use as a bastion server.
Traffic metrics	View CloudWatch metrics for the NAT gateway.	View CloudWatch metrics for the instance.
Timeout behavior	When a connection times out, a NAT gateway returns an RST packet to any resources behind the NAT gateway that attempt to continue the connection (it does not send a FIN packet).	When a connection times out, a NAT instance sends a FIN packet to resources behind the NAT instance to close the connection.
IP fragmentation	Supports forwarding of IP fragmented packets for the UDP protocol. Does not support fragmentation for the TCP and ICMP protocols. Fragmented packets for these protocols will get dropped.	Supports reassembly of IP fragmented packets for the UDP, TCP, and ICMP protocols.


AWS Account
Region-N.Virginia
Virtual Private Cloud (myVPC)
myIGW
us-east-1a
us-east-1b
us-east-1c
172.16.0.0
172.16.1.0
172.16.2.0
RouteTable
Public Subnet 1a
172.16.1.0/24
NAT gateway
Elastic IP address
Public Subnet 1b
172.16.4.0/24
Public Subnet 1c
172.16.7.0/24
Private Subnet 1a
172.16.2.0/24
Private Subnet 1b
172.16.5.0/24
Private Subnet 1c
172.16.8.0/24
172.16.0.0
172.16.1.0
172.16.2.0
RouteTable

Solution Architect Cases

1 You would like to provide Internet access to your EC2 instances in private subnets with IPv4 while making sure this solution requires the least amount of administration and scales seamlessly. What should you use?

NAT Gateway

2 We want to setup an encrypted connection from your local office to your VPC on AWS using the internet connection provided by your ISP. What is your advice?

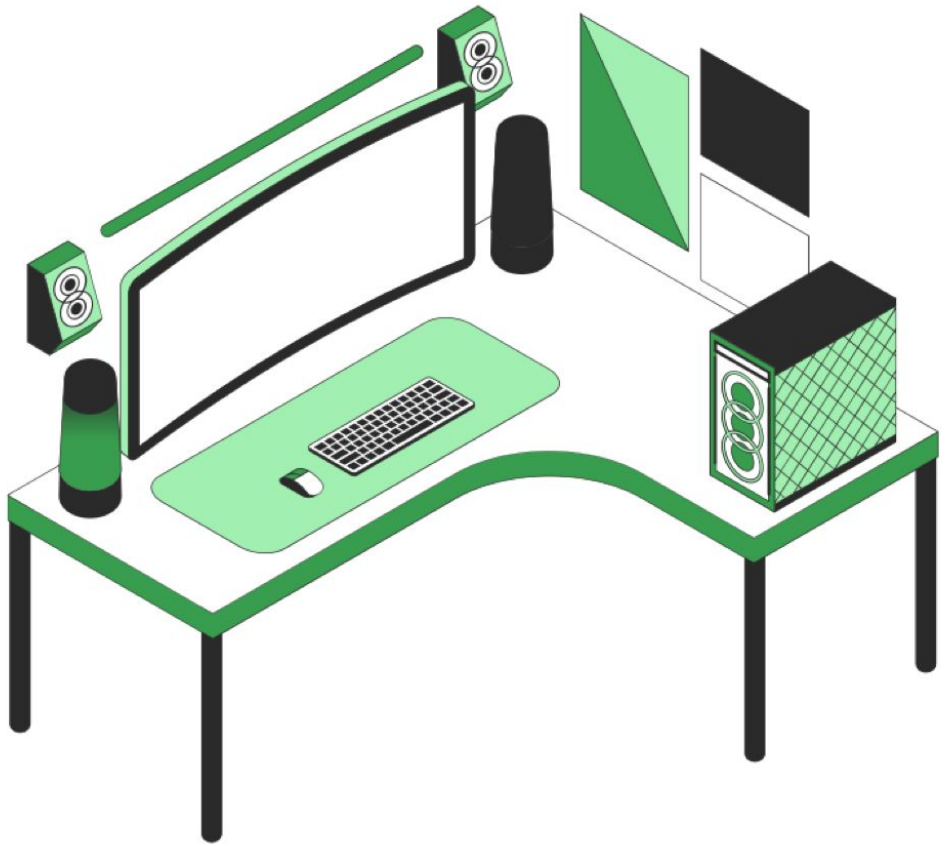
Consider VPN

3 You need to set up a dedicated connection between your on-premises corporate datacenter and AWS Cloud. This connection must be private, consistent, and traffic must not travel through the Internet. Which AWS service should you use?

AWS Direct Connect

4 You have a VPC. You created a new private subnet and created a route table with a path to a NAT gateway. However, EC2 instances launched into this subnet are not able to reach the Internet. Security Groups for the EC2 instances are setup correctly. What is the most likely explanation?

You need to assign the new route table in order for the instances to see the route to the NAT gateway.



Do you have any questions?

Send it to us! We hope you learned something new.