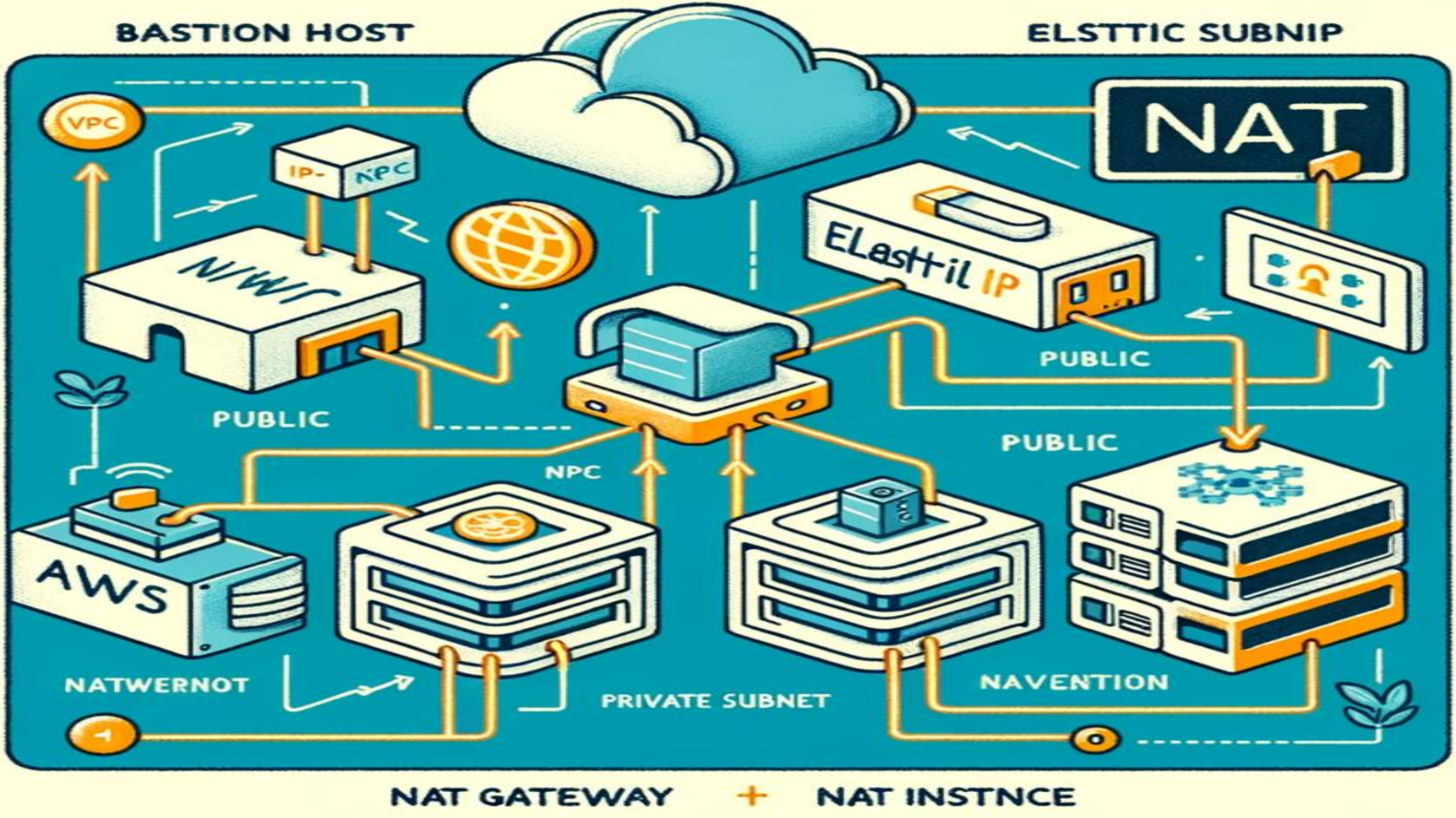
DATE	:	20.02.2025
DT/NT	:	DT
LESSON	:	AWS
SUBJECT	:	**VPC-2** Bastion Host, Elastic IP, NAT Gateway, NAT Instance
BATCH	:	B 303

AWS-DEVOPS

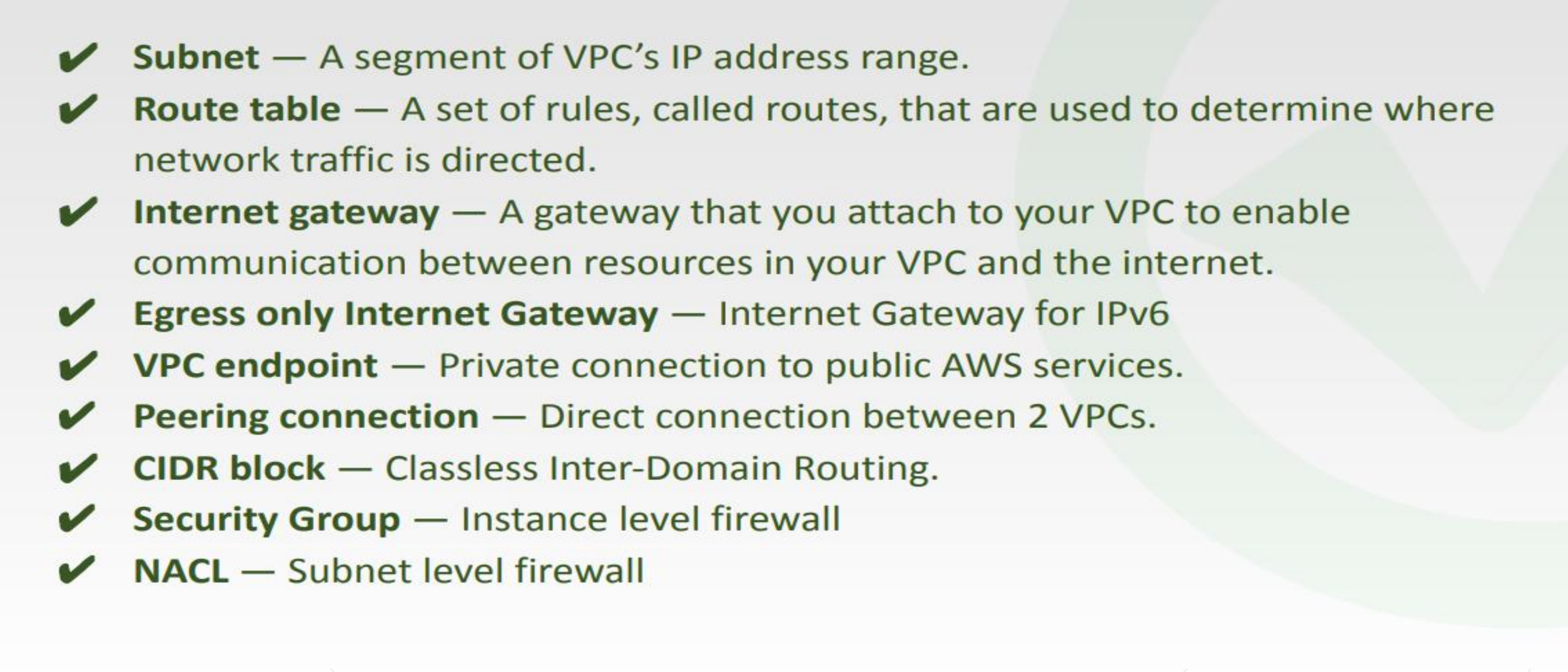
TECHPRO
EDUCATION

techproeducation.com

+1 (585) 304 29 59

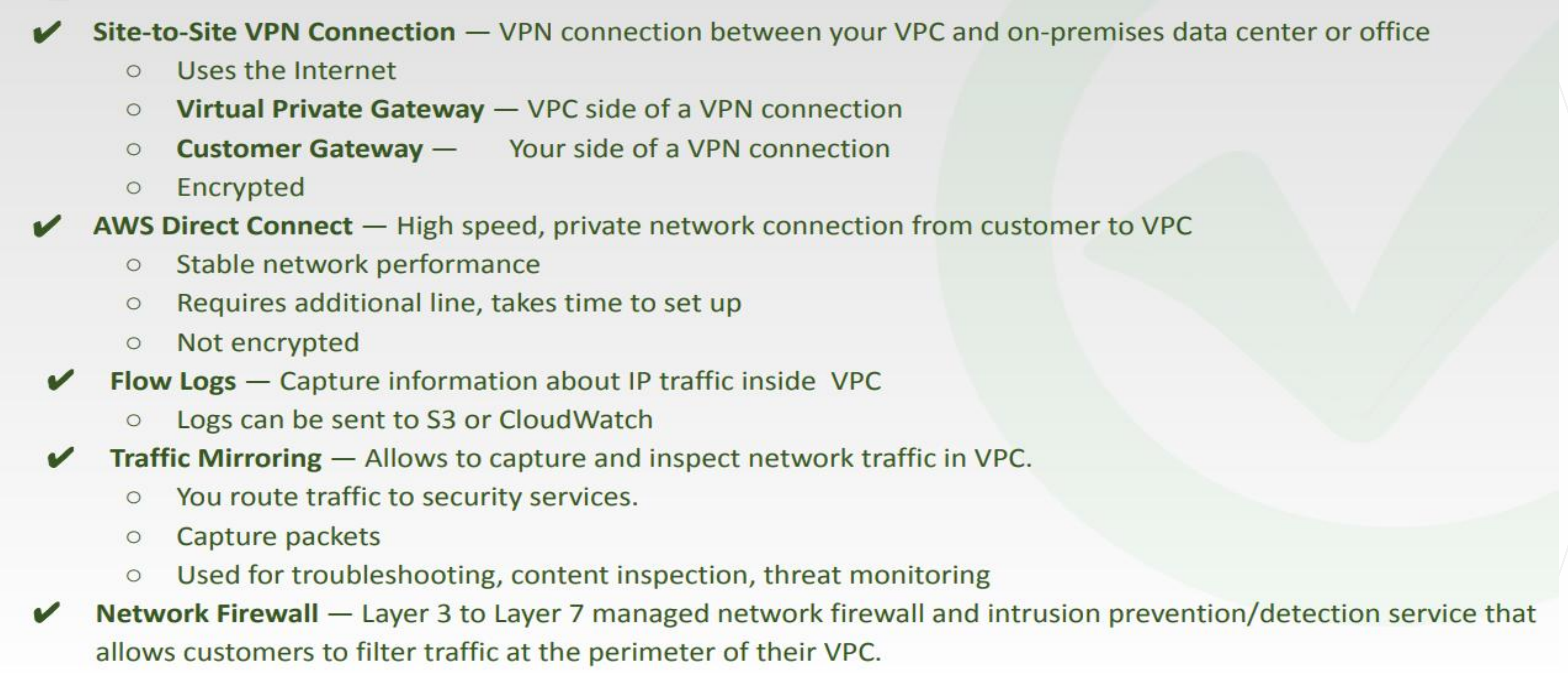

BASTION HOST
ELSTTIC SUBNIP
VPC
IP-
NPC
NAT
NIWI
ELASTTIL IP
PUBLIC
PUBLIC
PUBLIC
NPC
AWS
NATWERNOT
PRIVATE SUBNET
NAVENTION
NAT GATEWAY
+
NAT INSTNCE

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

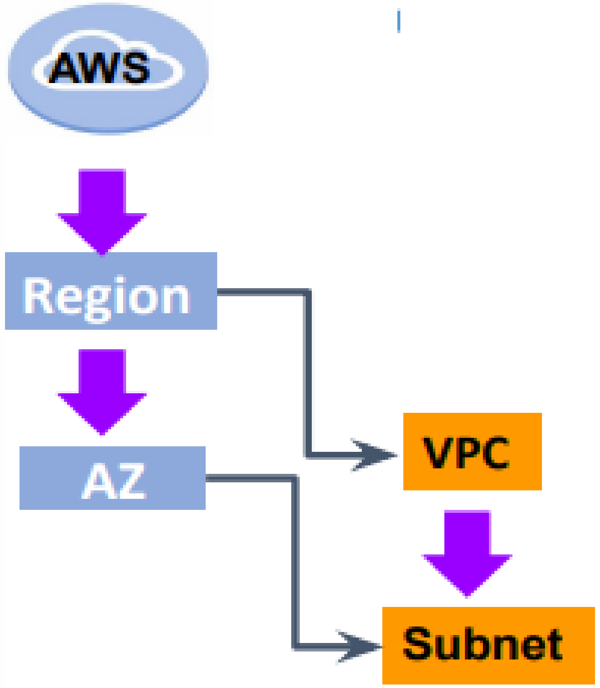
- Logs can be sent to S3 or CloudWatch

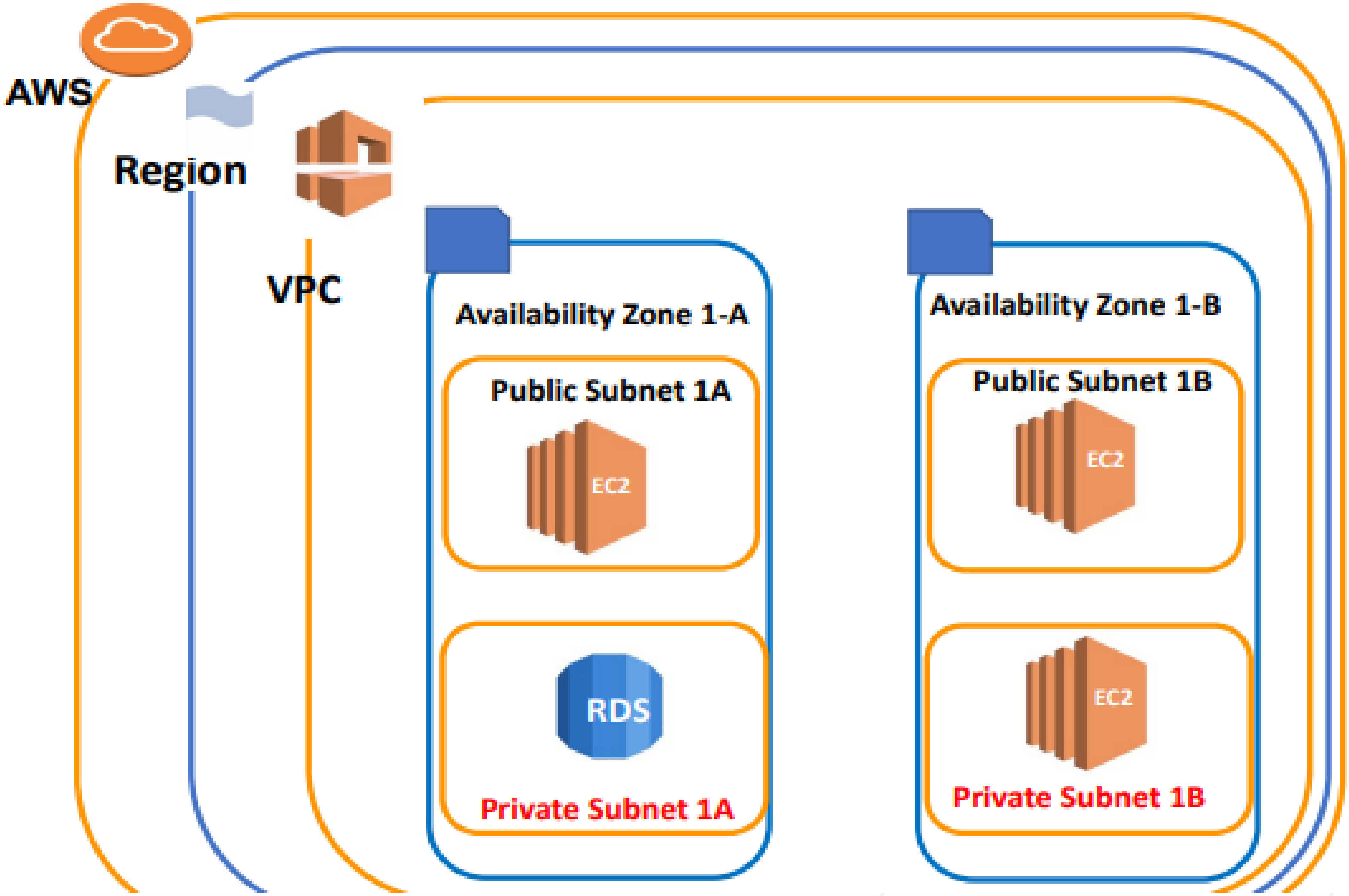
✔ **Traffic Mirroring** — Allows to capture and inspect network traffic in VPC.

- 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.

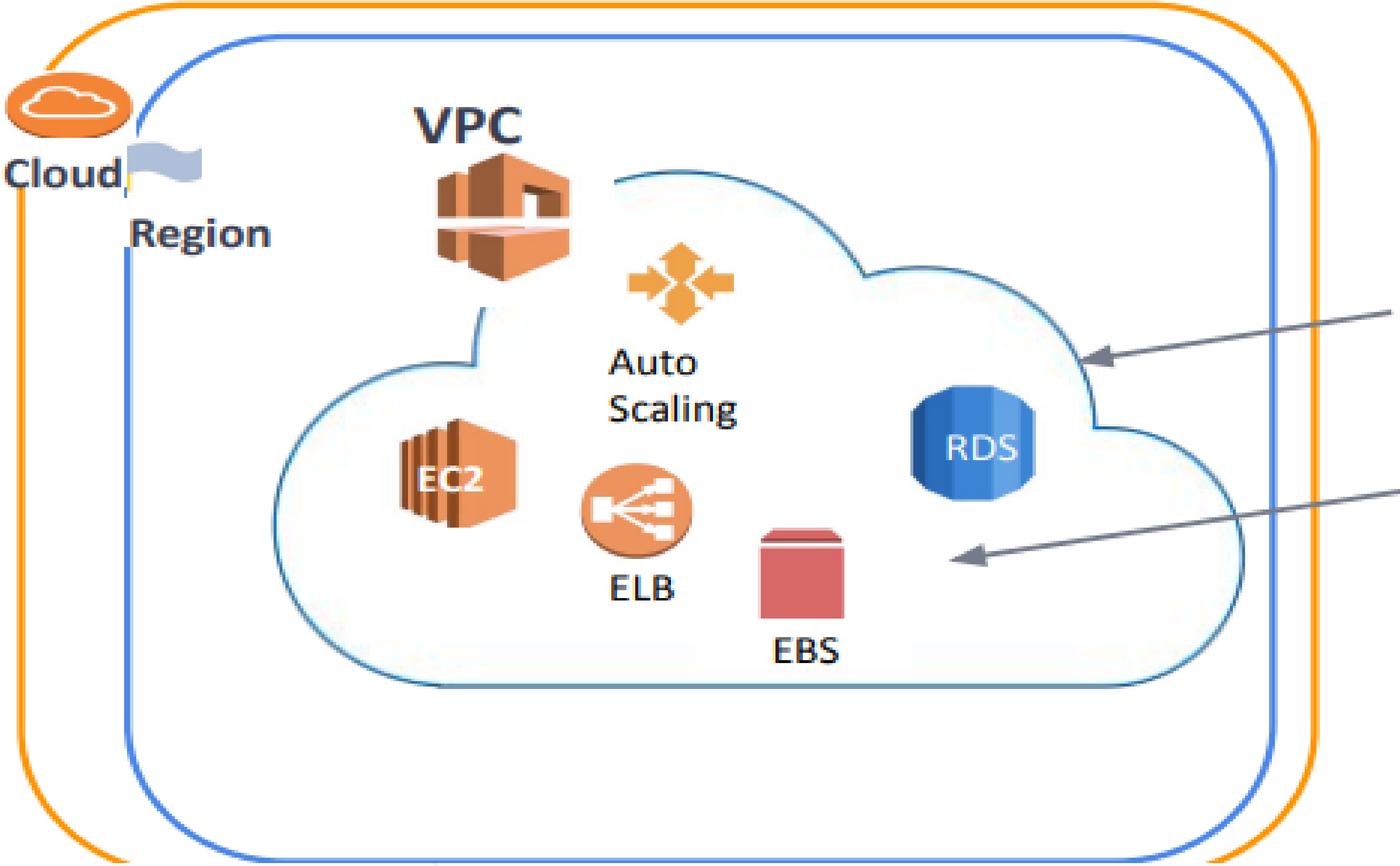
Region,VPC, AZ and Subnets





Introduction to VPC

What is VPC?

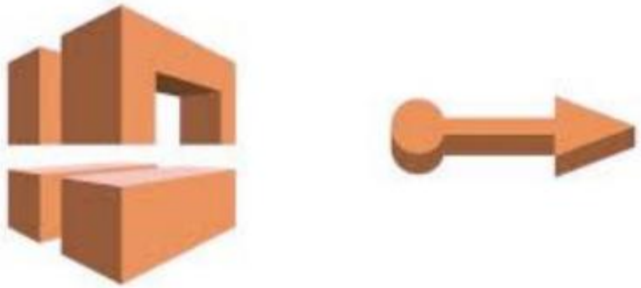


Amazon Virtual Private Cloud (Amazon VPC) is a logically isolated area of the AWS cloud where you can launch AWS resources in a virtual network that you define.

Table of Contents

- VPC Solutions
  - Elastic IP
  - Bastion Host /Jump Box
  - NAT Gateway
  - NAT Instance

Elastic IP



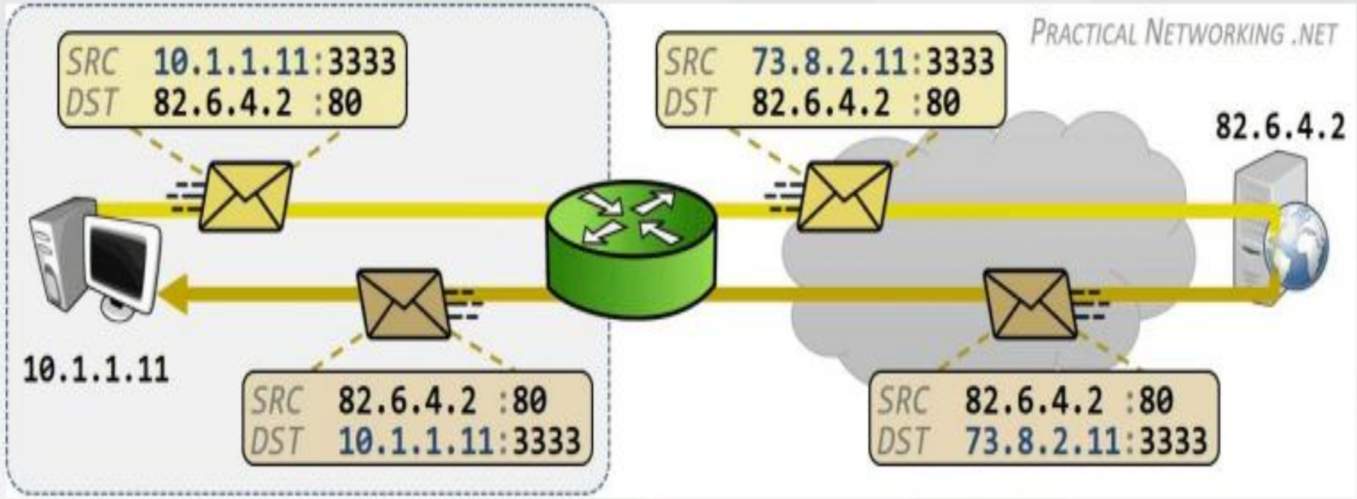
An Elastic IP address is a Static IPv4 Address

Legal requirement for some applications or license policy to may render you to use static IP. In addition, some AWS components/services such as NAT Gateway and Route 53 may need Elastic IP.

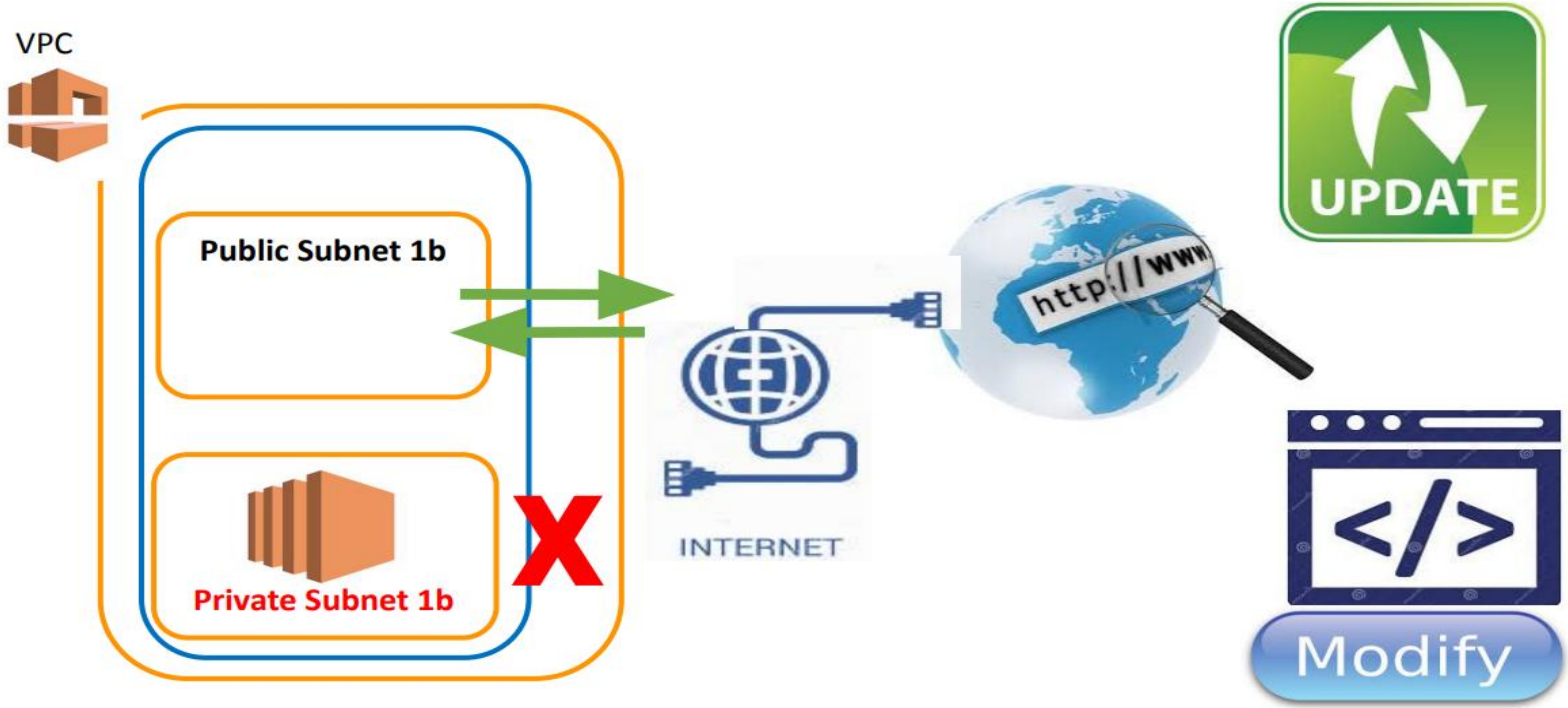
Elastic IP is free of charge as long as they are being used. However, you will be charged for each EIP if you reserve and not use it.

NAT

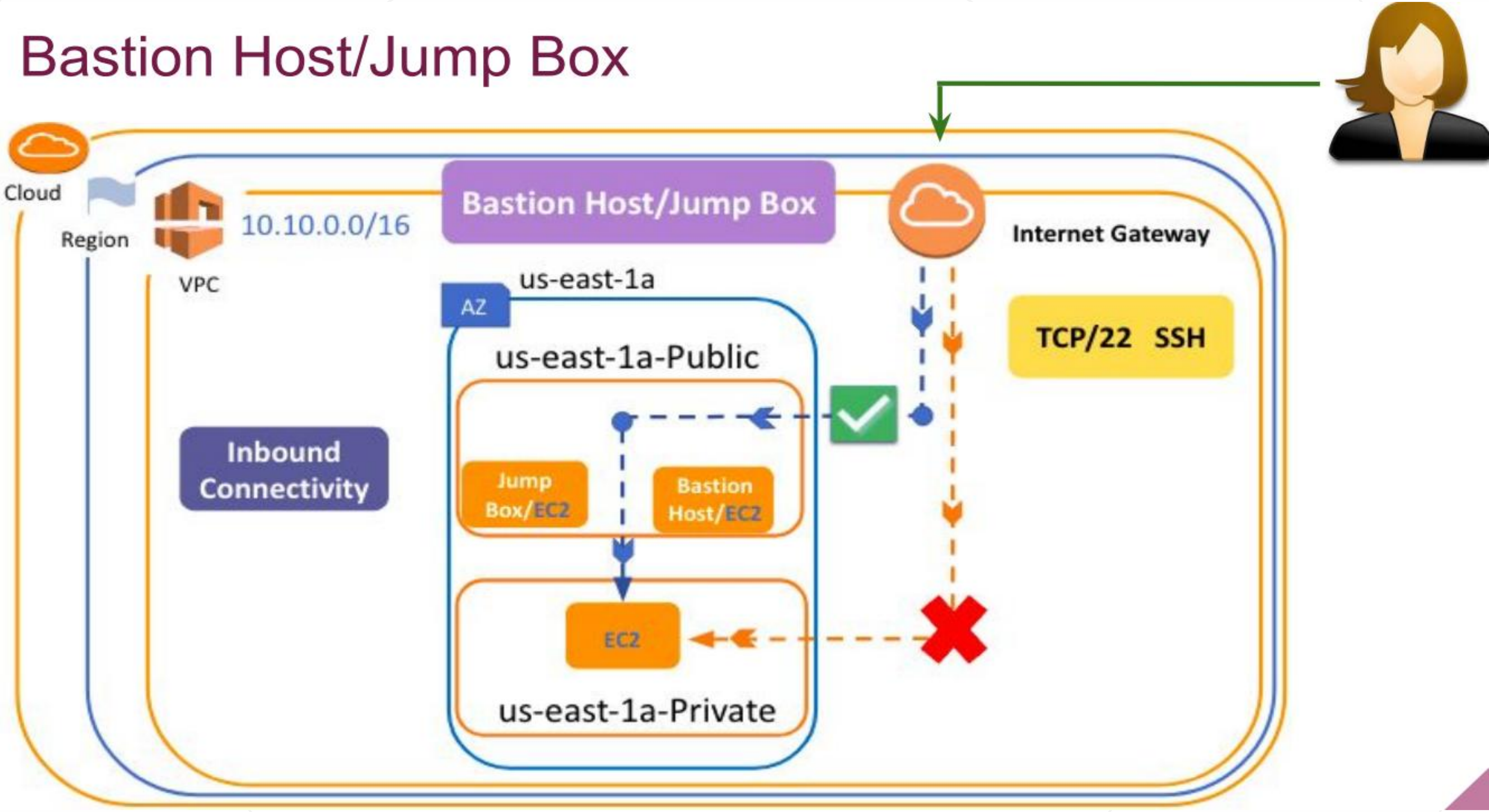
- NAT stands for network address translation. It's a way to **map multiple private addresses** inside a local network **to a public IP address** before transferring the information onto the internet.
- **Mapping** is done by **changing the header of IP packets** while in transit via a router. This helps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



Why NAT Gateway, NAT Instance and Bastion Host?

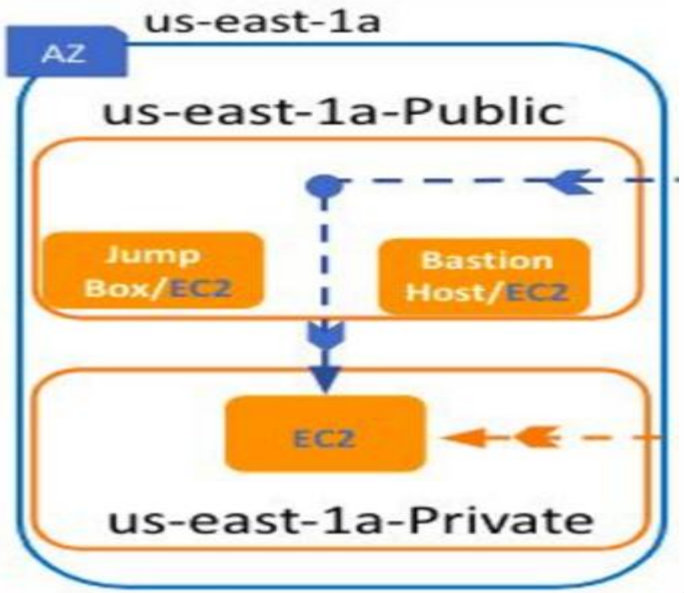


Bastion Host/Jump Box

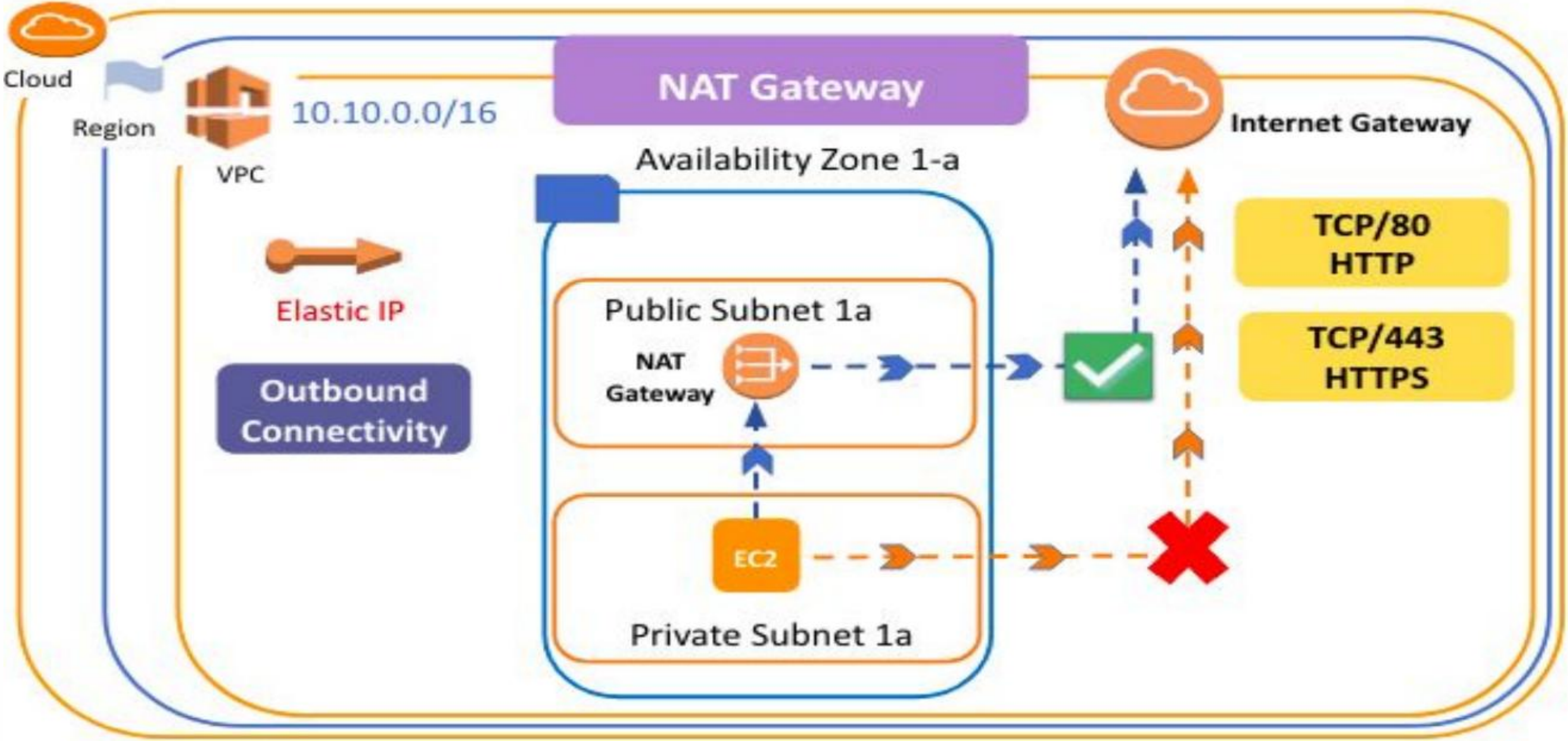


Bastion Host/Jump Box

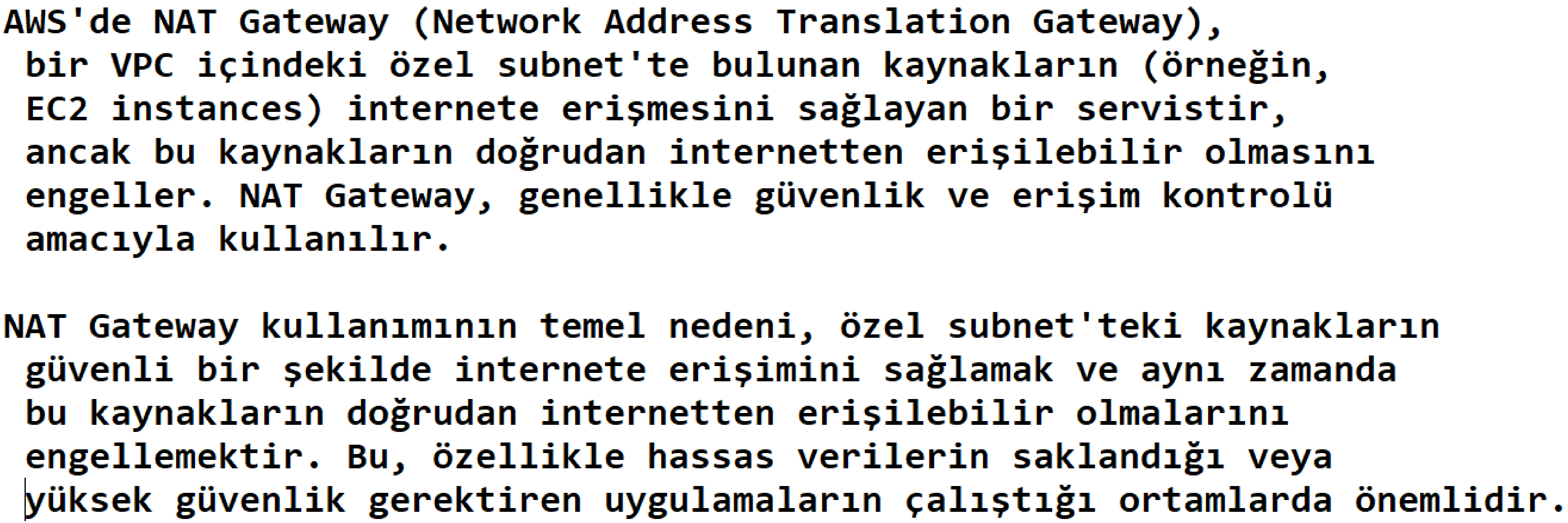
Bastion host, bir ağın güvenlik düzenlemesinde, dış dünyadan gelen bağlantıları kabul eden ve genellikle güvenlik amaçlı bir sunucudur. AWS gibi bulut ortamlarında bastion host'lar, genellikle özel ağlarda (VPC içindeki özel subnetlerde) bulunan sunuculara güvenli bir şekilde erişim sağlamak için kullanılır. Bastion host'ların temel özellikleri ve işlevleri şunlardır:



NAT Gateway


Cloud
Region
VPC
10.10.0.0/16
NAT Gateway
Internet Gateway
Availability Zone 1-a
Elastic IP
Outbound Connectivity
Public Subnet 1a
NAT Gateway
TCP/80 HTTP
TCP/443 HTTPS
EC2
Private Subnet 1a

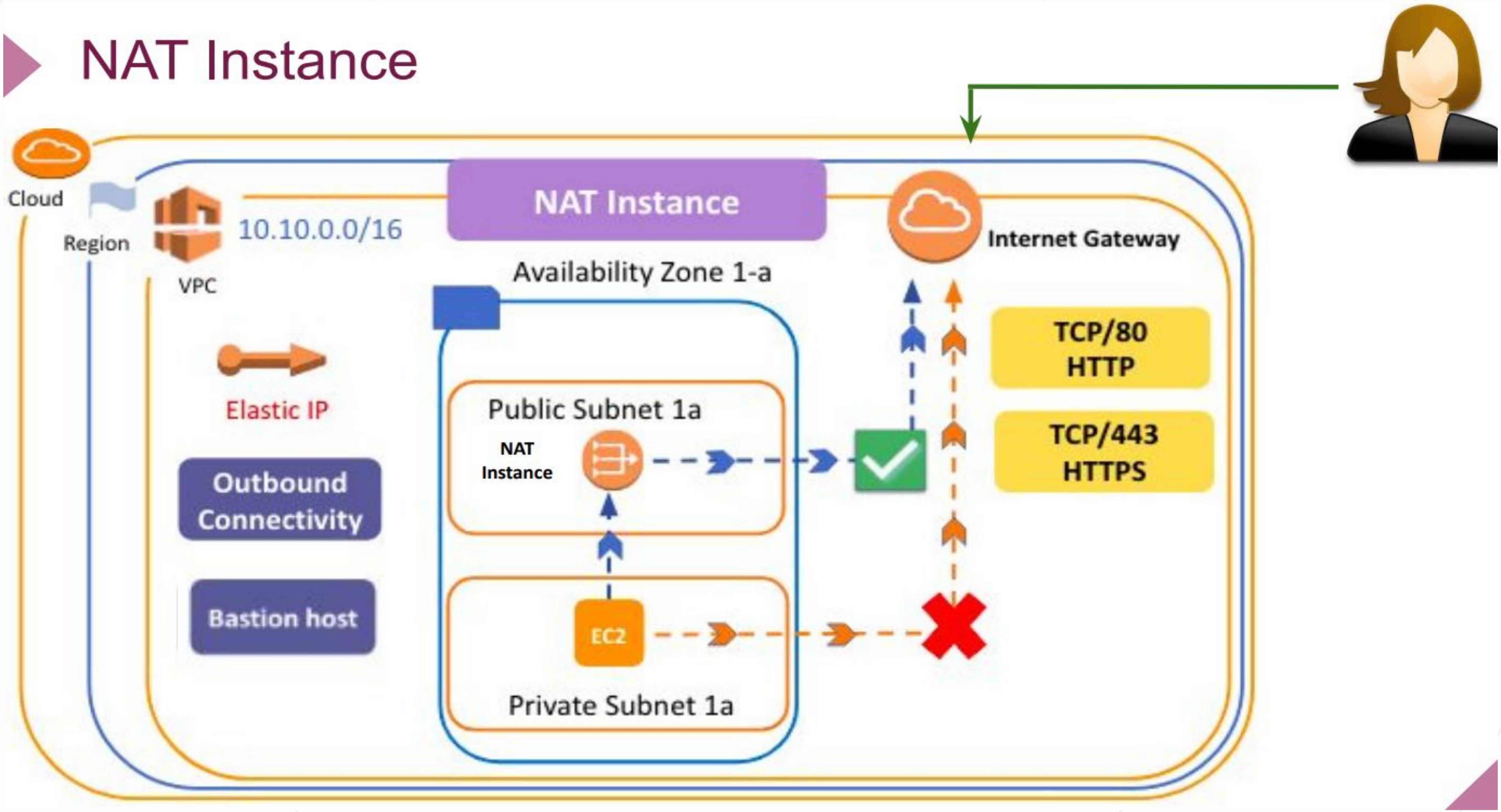
NAT Gateway (Network Address Translation Gateway)



AWS'de NAT Gateway (Network Address Translation Gateway), bir VPC içindeki özel subnet'te bulunan kaynakların (örneğin, EC2 instances) internete erişmesini sağlayan bir servistir, ancak bu kaynakların doğrudan internetten erişilebilir olmasını engeller. NAT Gateway, genellikle güvenlik ve erişim kontrolü amacıyla kullanılır.

NAT Gateway kullanımının temel nedeni, özel subnet'teki kaynakların güvenli bir şekilde internete erişimini sağlamak ve aynı zamanda bu kaynakların doğrudan internetten erişilebilir olmalarını engellemektir. Bu, özellikle hassas verilerin saklandığı veya yüksek güvenlik gerektiren uygulamaların çalıştığı ortamlarda önemlidir.

NAT Instance

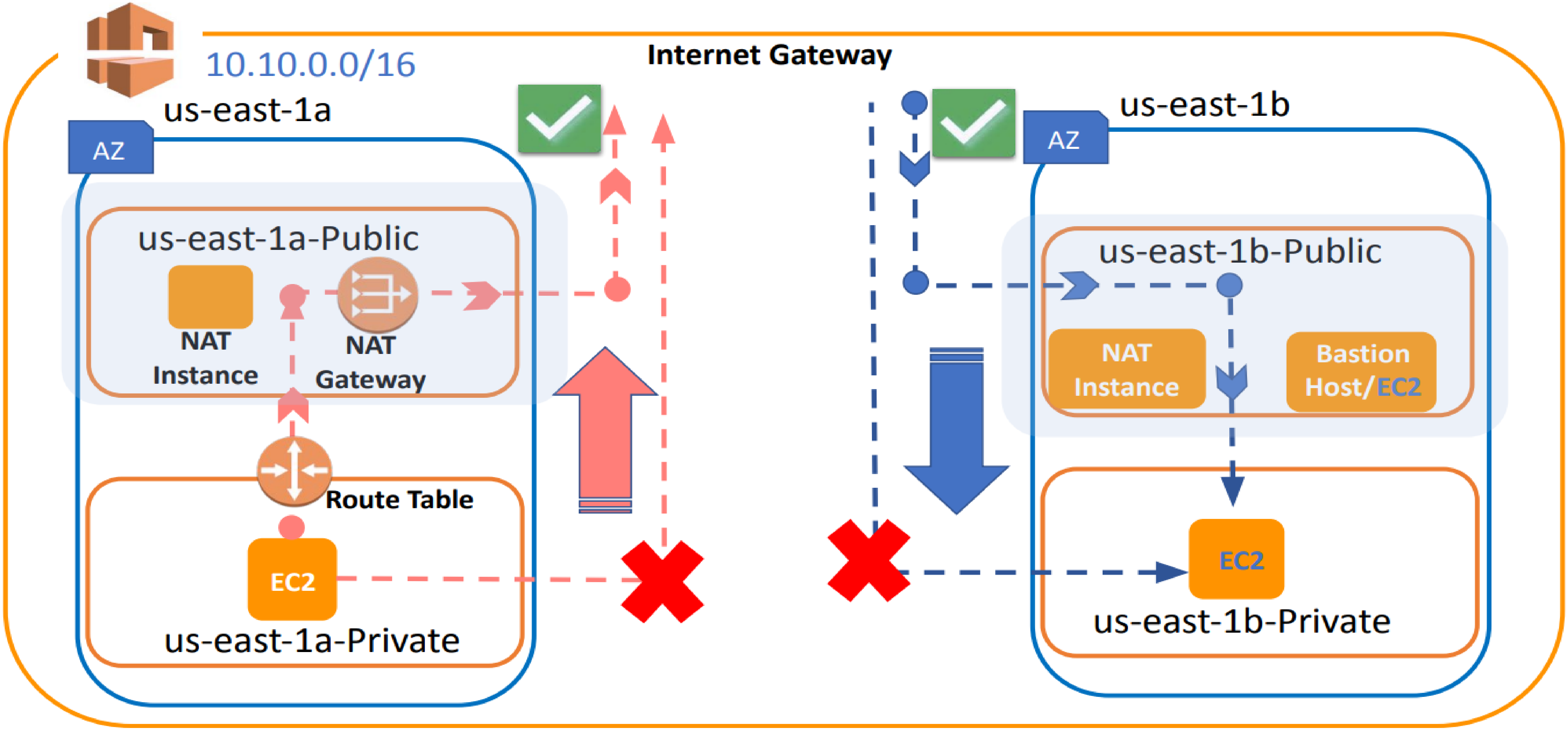


NAT Instance

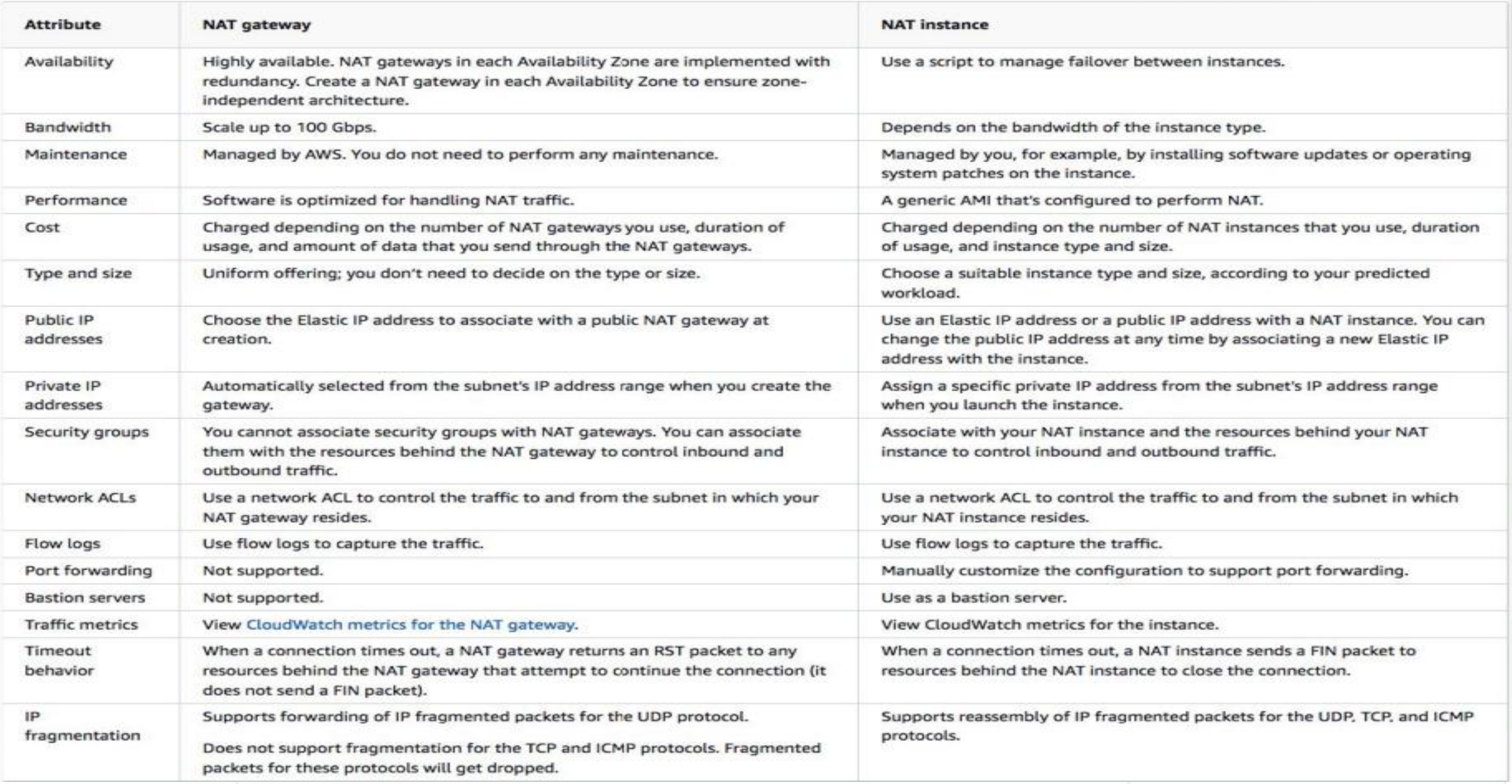
In AWS, a **NAT Instance** (Network Address Translation) is an **EC2 instance managed by the user** that performs the network address translation function. A NAT Instance is **primarily used within a VPC (Virtual Private Cloud)** to allow resources in **private subnets** (such as EC2 instances) to access the internet while preventing inbound connections from the internet from reaching these resources. The main functions and characteristics of NAT Instances are as follows:

The **primary reason** for using a **NAT Instance** is to enable **secure internet access for resources in private subnets** while ensuring that **these resources remain inaccessible from the internet**. However, due to the additional **management overhead and configuration requirements**, AWS's **managed service, NAT Gateway,** is preferred in many cases.

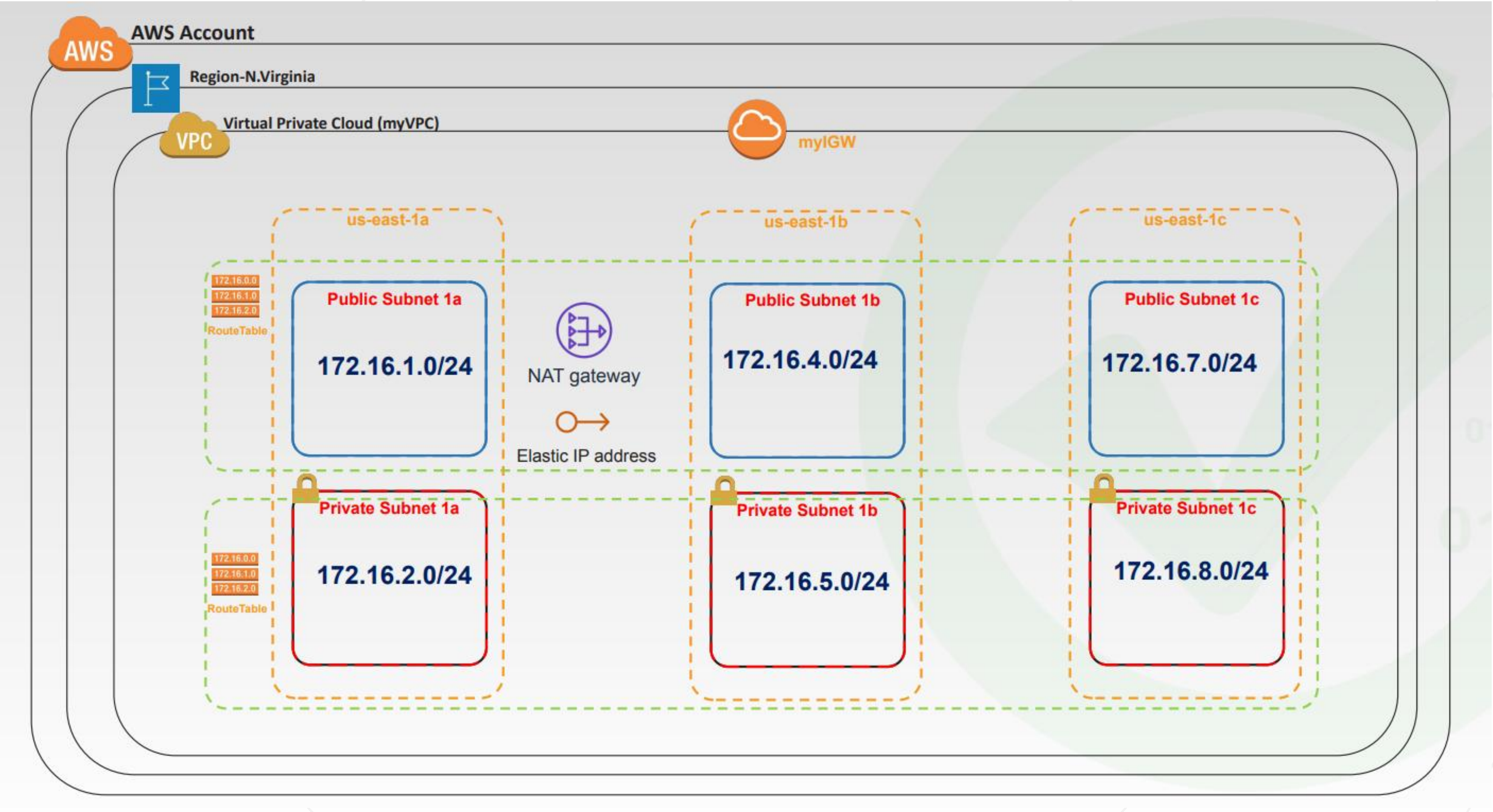
NAT Gateway vs. Bastion Host/Jump Box

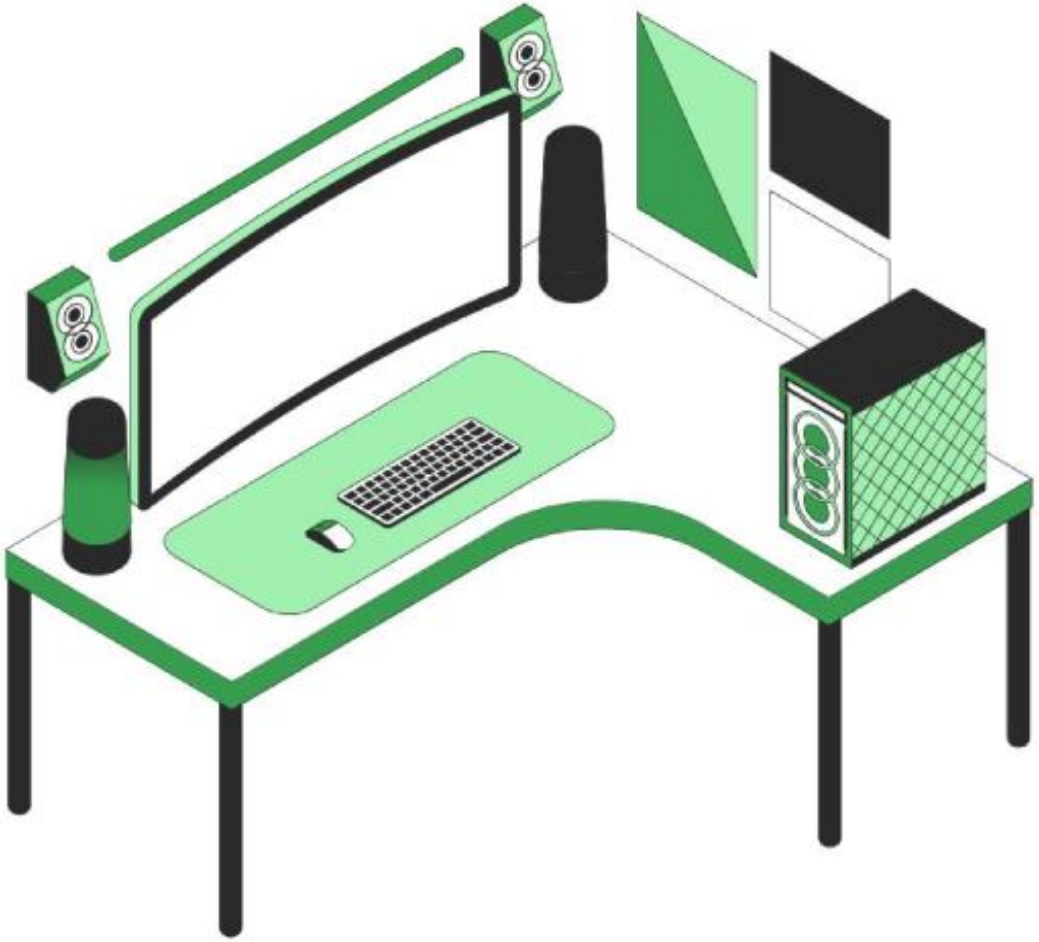


Nat Gateway vs Nat Instance



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
AWS Account
Region-N.Virginia
VPC
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
172.16.0.0
172.16.1.0
172.16.2.0
RouteTable
Private Subnet 1a
172.16.2.0/24
Private Subnet 1b
172.16.5.0/24
Private Subnet 1c
172.16.8.0/24



Do you have any questions?

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