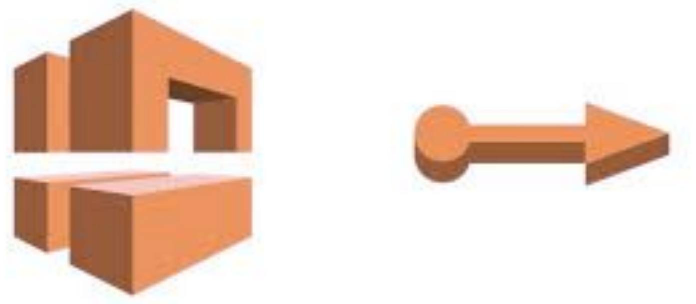
Amazon VPC-2

CLARUSWAY
WAY TO REINVENT YOURSELF

Table of Contents

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

Elastic IP

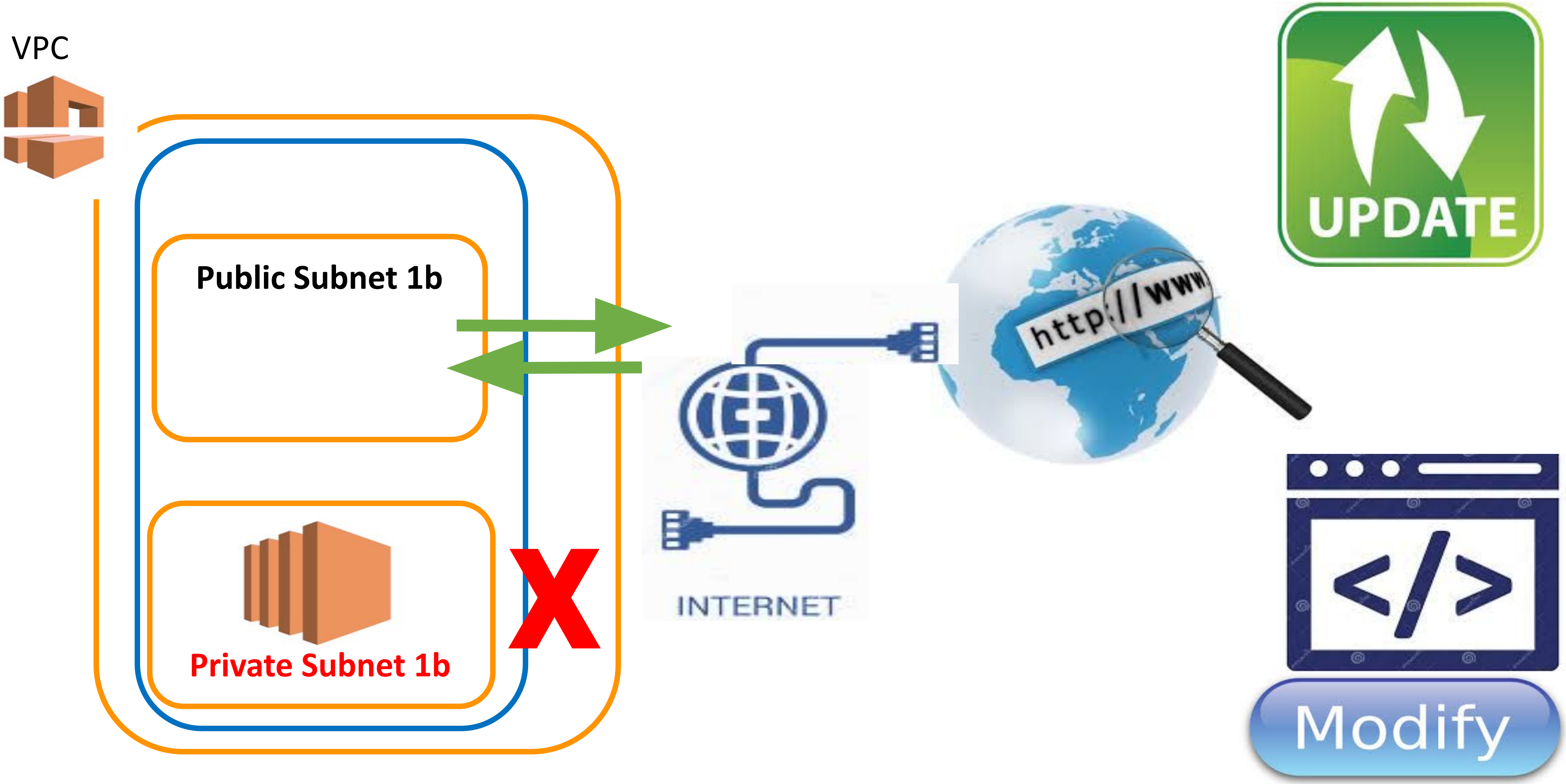


- An Elastic IP address is a Static IPv4 Address

- 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.

Why NAT Gateway, NAT Instance and Bastion Host?



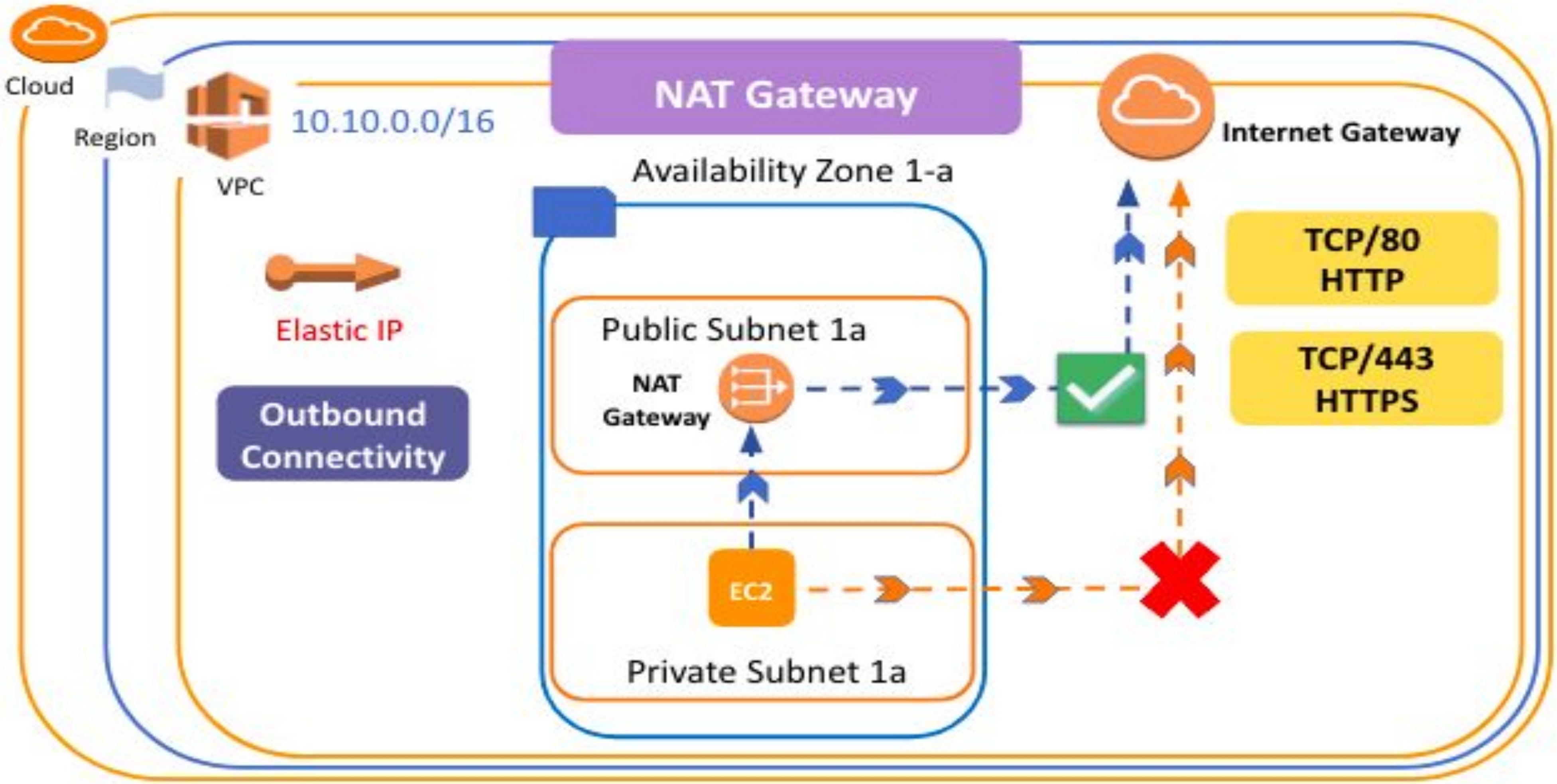
Logic of NAT Gateway

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.

When you create a NAT gateway, you specify one of the following connectivity types:

- **Public** – (Default) Instances in private subnets can connect to the internet through a public NAT gateway, but cannot receive unsolicited inbound connections from the internet.
- **Private** – Instances in private subnets can connect to other VPCs or your on-premises network through a private NAT gateway.

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
EC2
Private Subnet 1a
TCP/80
HTTP
TCP/443
HTTPS

Logic of NAT Instance

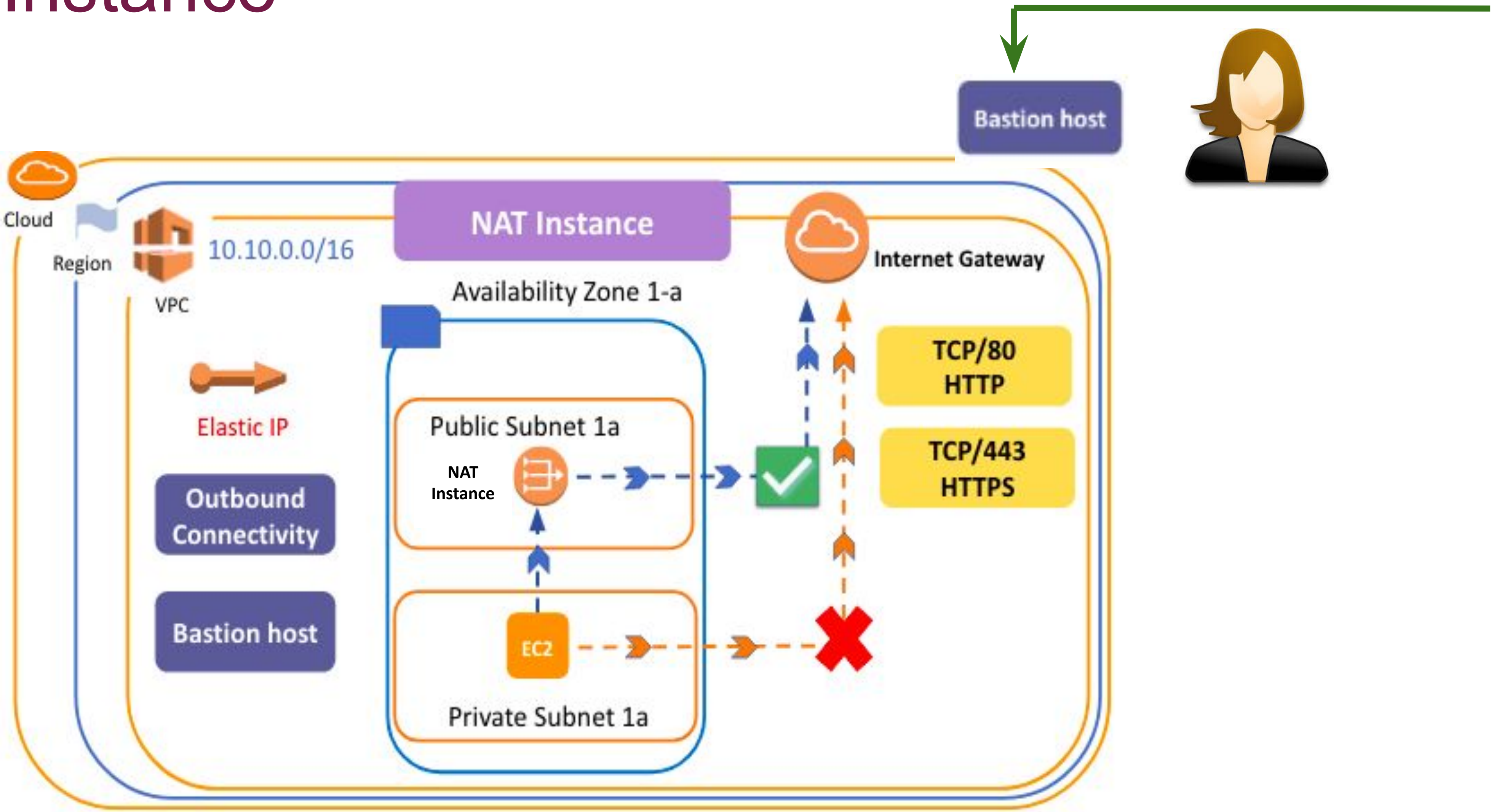
We can launch an EC2 NAT instance from a NAT AMI

NAT instance/NAT gateway should be launched in a public subnet to enable instances in the private subnet to initiate outbound IPv4 traffic to the internet or other AWS services, but prevent the instances from receiving inbound traffic initiated on the internet.

Disable source/destination checks

Each EC2 instance performs source/destination checks by default. This means that the instance must be the source or destination of any traffic it sends or receives. However, a NAT instance must be able to send and receive traffic when the source or destination is not itself. Therefore, we must disable source/destination checks on the NAT instance.

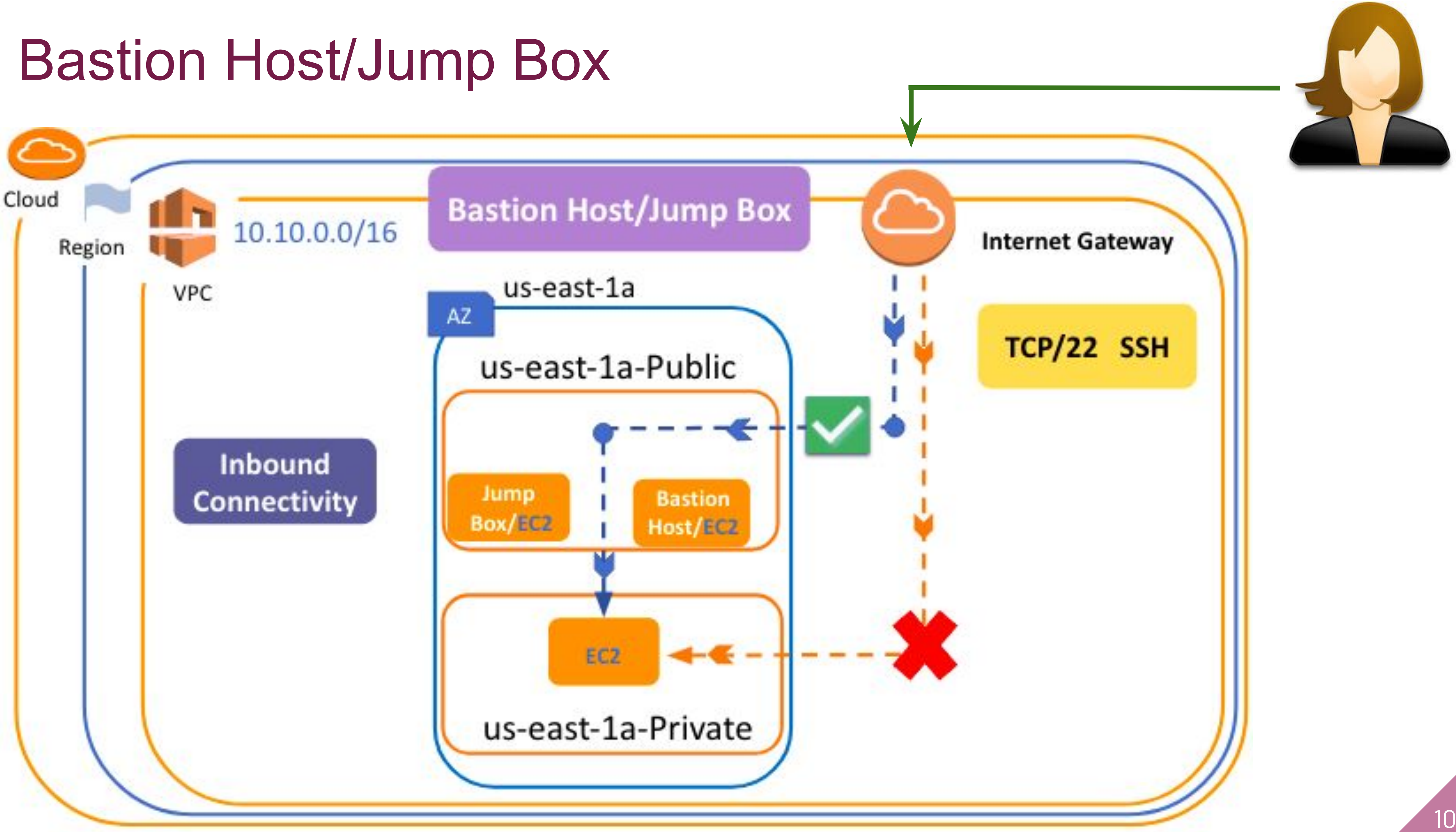
NAT Instance



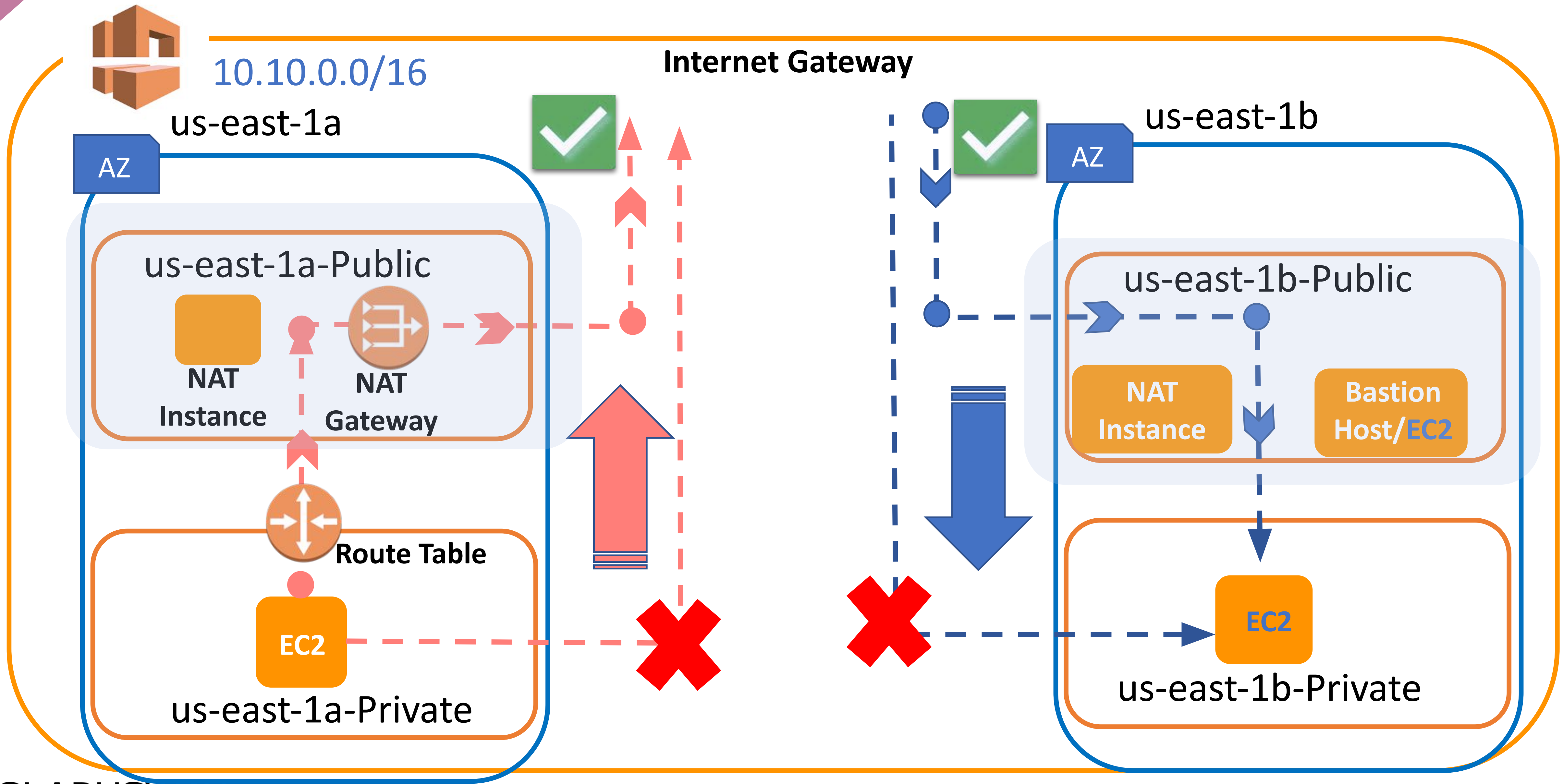
Logic of Bastion Host

- A bastion host is a server whose purpose is to provide access to a private network from an external/internal network, such as the Internet
- Because of its exposure to potential attack, a bastion host must minimize the chances of penetration
- For example, you can use a bastion host to mitigate the risk of allowing SSH connections from an external network to the Linux instances launched in a private subnet of your Amazon Virtual Private Cloud (VPC)

Bastion Host/Jump Box



NAT Gateway vs. Bastion Host/Jump Box



CLARUSWAY
WAY TO REINVENT YOURSELF

Using SSH Agent Forwarding

- It's a program that runs in the background and keeps your SSH key loaded into memory, so that you don't need to enter your passphrase every time you need to use the key
- The nifty thing is, you can choose to let servers access your local ssh-agent as if they were already running on the server
- This is sort of like asking a friend to enter their password so that you can use their computer

THANKS!

Any questions?

You can find me at:

- @sumod
- sumod@clarusway.com