VPC-PART-1

- Introduction to VPC
- VPC Basic Components

Create VPC

- *Name tag*: **clarus-vpc-a**
- *IPv4 CIDR block*: **10.7.0.0/16**

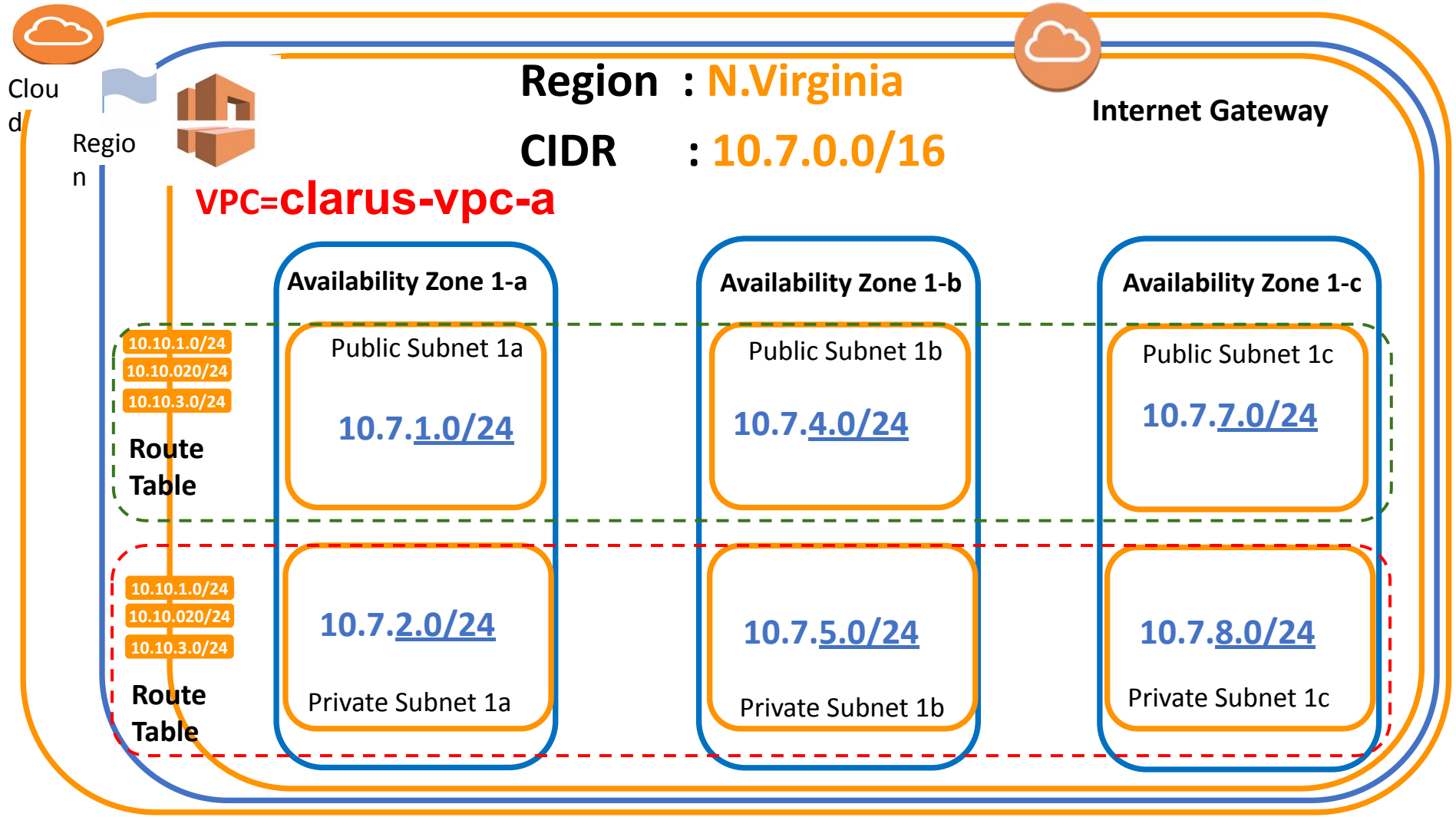
Create IGW

IGW Action Menu:
Attach IGW to VPC

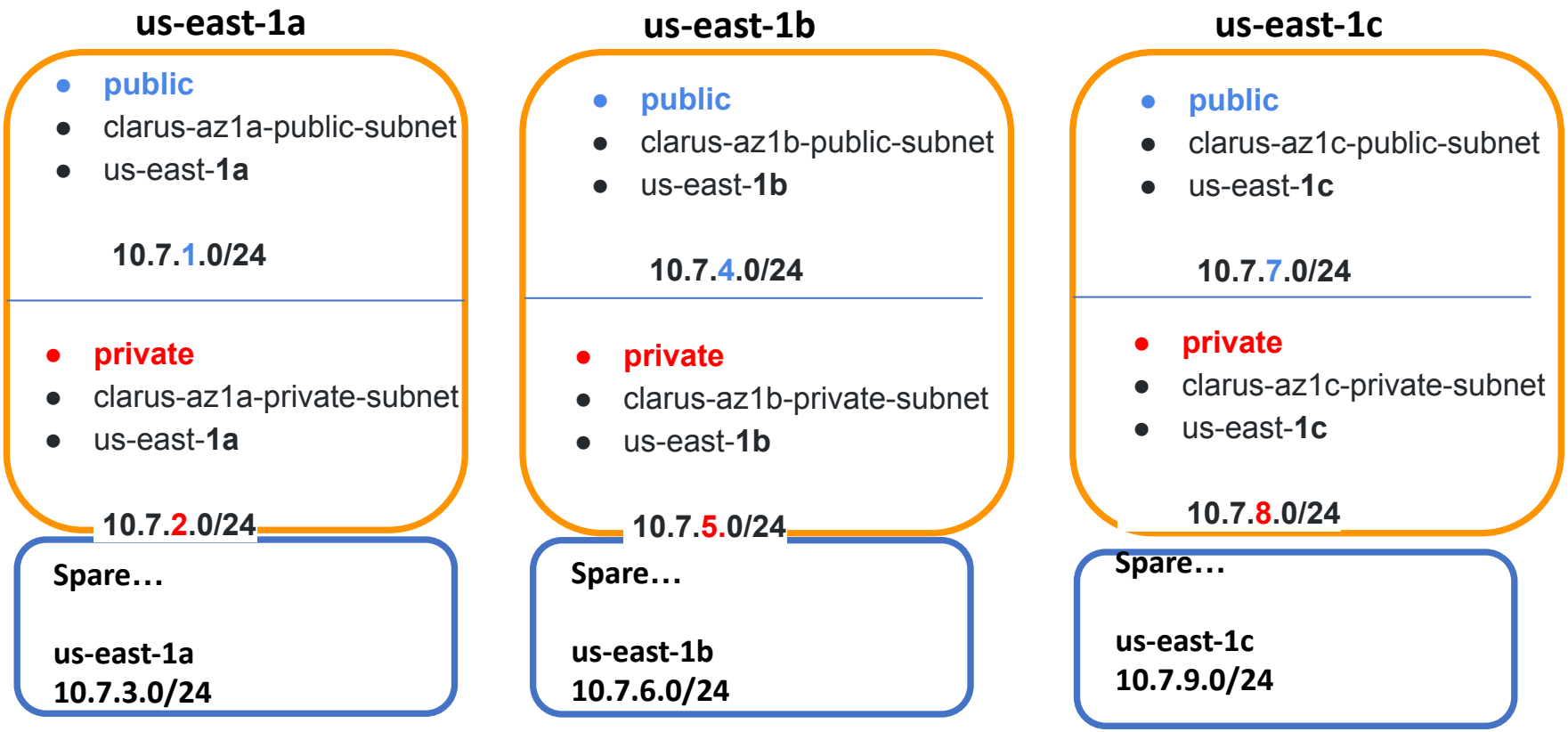
Set the VPC Route Table:
00000:/0 > IGW

VPC Action Menu:
Edit DNS Hostname

Name Default Route Table: default-labvpc


Cloud
Region
Region : N.Virginia
CIDR : 10.7.0.0/16
Internet Gateway
VPC=clarus-vpc-a
Availability Zone 1-a
Availability Zone 1-b
Availability Zone 1-c
10.10.1.0/24
10.10.020/24
10.10.3.0/24
Route Table
Public Subnet 1a
10.7.1.0/24
Public Subnet 1b
10.7.4.0/24
Public Subnet 1c
10.7.7.0/24
10.10.1.0/24
10.10.020/24
10.10.3.0/24
Route Table
10.7.2.0/24
Private Subnet 1a
10.7.5.0/24
Private Subnet 1b
10.7.8.0/24
Private Subnet 1c

- *Name tag*: **clarus-vpc-a**
- *IPv4 CIDR block*: **10.7.0.0/16**



VPC CIDR IP POOL

AWS PUBLIC IP POOL

10.7.0.0/16 = 65000 IP

VPC

10.7.1.0/32

10.7.2.0/32

175.0.0.1/32

Private Subnet

Public Subnet

Connectivity

Virtual Private Cloud (VPC) Info

VPC that defines the virtual networking environment for this DB instance.

Default VPC (vpc-d8715da2)

Only VPCs with a corresponding DB subnet group are listed.

After a database is created, you can't change the VPC selection.

▼ Additional connectivity configuration

Subnet group Info

DB subnet group that defines which subnets and IP ranges the DB instance can use in the VPC you selected.

default

Publicly accessible Info

- Yes
  Amazon EC2 instances and devices outside the VPC can connect to your database. Choose one or more VPC security groups that specify which EC2 instances and devices inside the VPC can connect to the database.
- No
  RDS will not assign a public IP address to the database. Only Amazon EC2 instances and devices inside the VPC can connect to your database.

Clou
d

Regio
n

VP
C

10.10.0.0/16

Local

2

Internet
Gateway

10.10.1.0/24
10.10.020/24
10.10.3.0/24

Route
Tables

1- All Subnets are associated with Default Route Table Implicitly

2- By default all subnets are PUBLIC !!!!!!

a.Local

b.0000/0 >>>>IGW

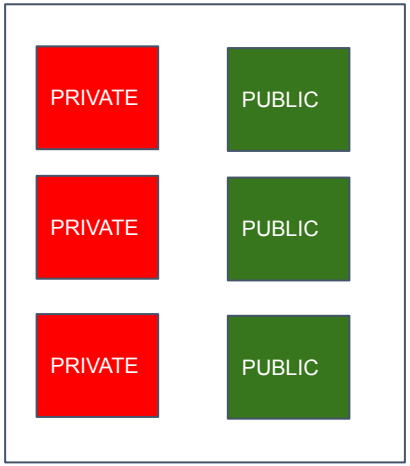
Conclusion

Current= 6 Public

Desired= 3 Public 3 Private

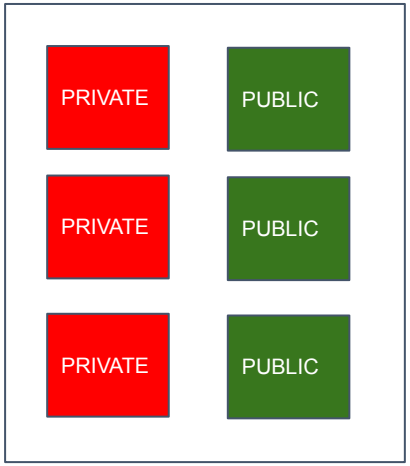
Option-1

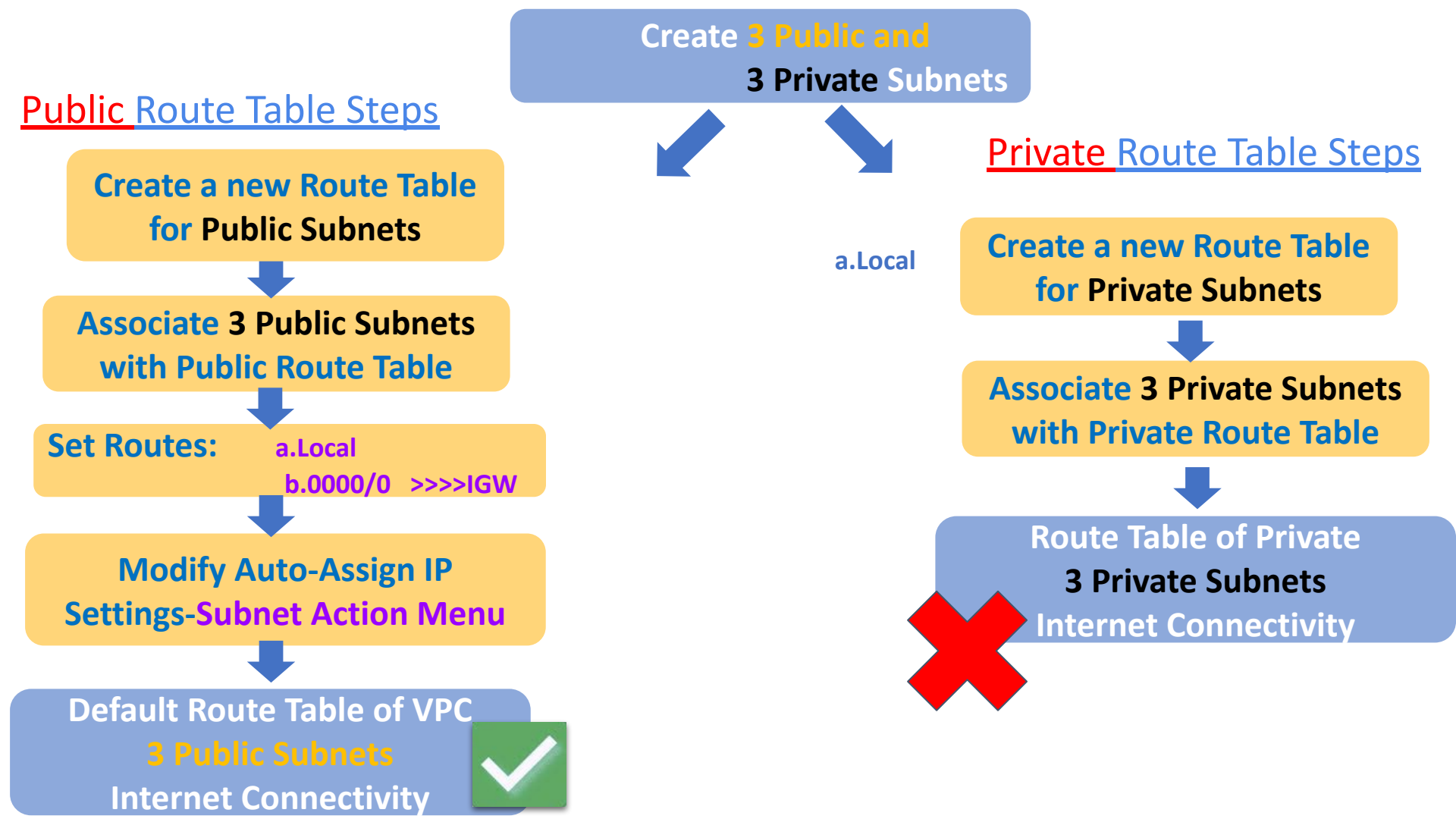
DEFAULT RT



Option-2

DEFAULT RT




Create 3 Public and
3 Private Subnets
Public Route Table Steps
Create a new Route Table
for Public Subnets
Associate 3 Public Subnets
with Public Route Table
Set Routes: a.Local
b.0000/0 >>>>IGW
Modify Auto-Assign IP
Settings-Subnet Action Menu
Default Route Table of VPC
3 Public Subnets
Internet Connectivity
a.Local
Private Route Table Steps
Create a new Route Table
for Private Subnets
Associate 3 Private Subnets
with Private Route Table
Route Table of Private
3 Private Subnets
Internet Connectivity

Launching an Instance

Create in Public Subnet

Create in Private Subnet

Private IP

VPC CIDR Pool

+

Public IP

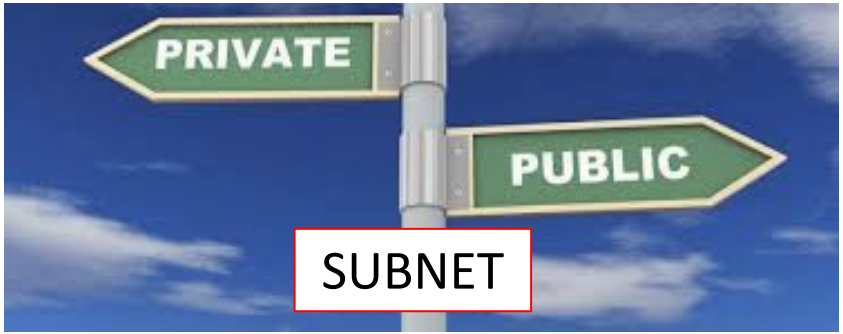
(Auto Assign IP)

AWS IP POOL

Private IP

VPC CIDR Pool

Route



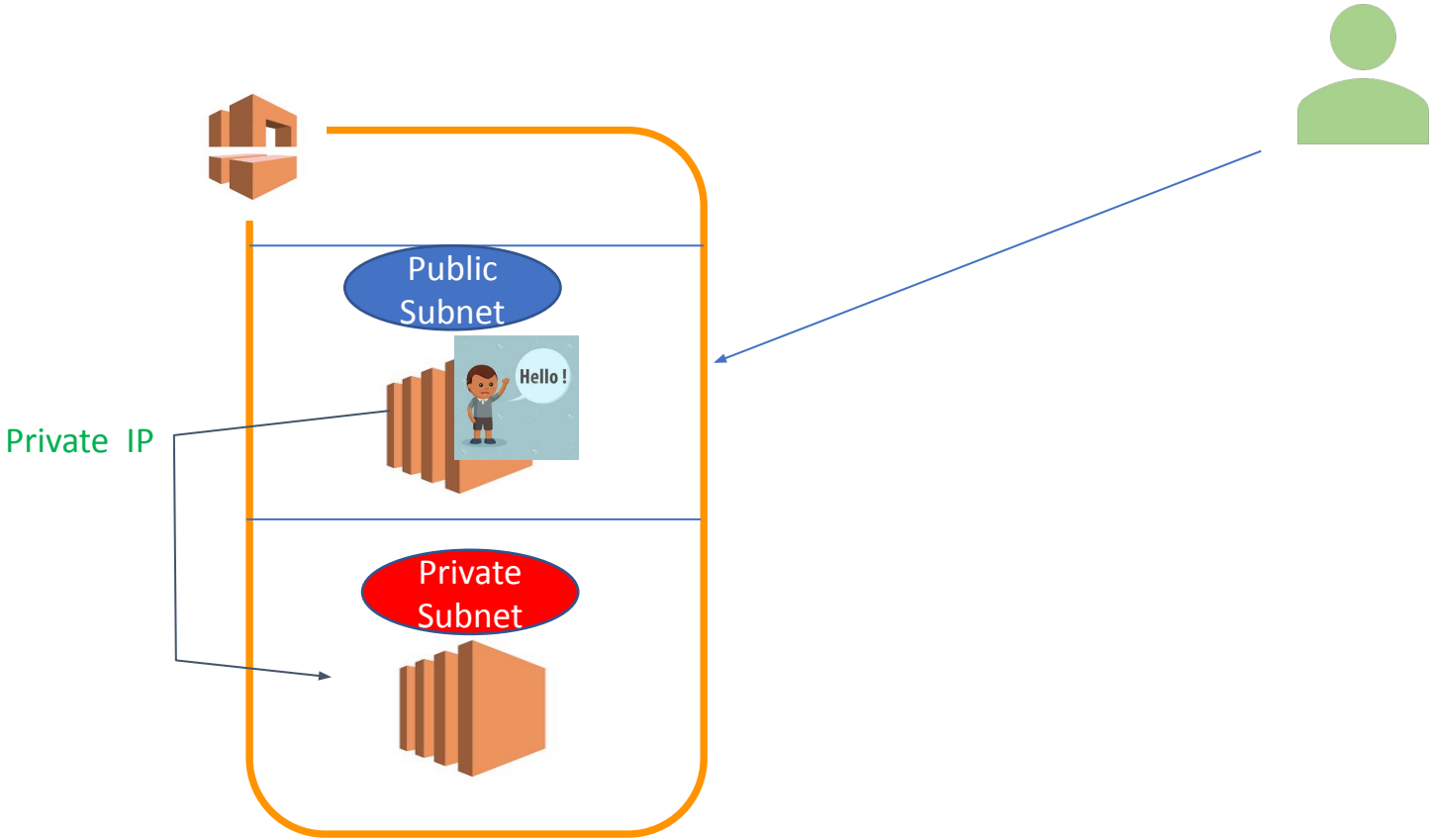
SUBNET

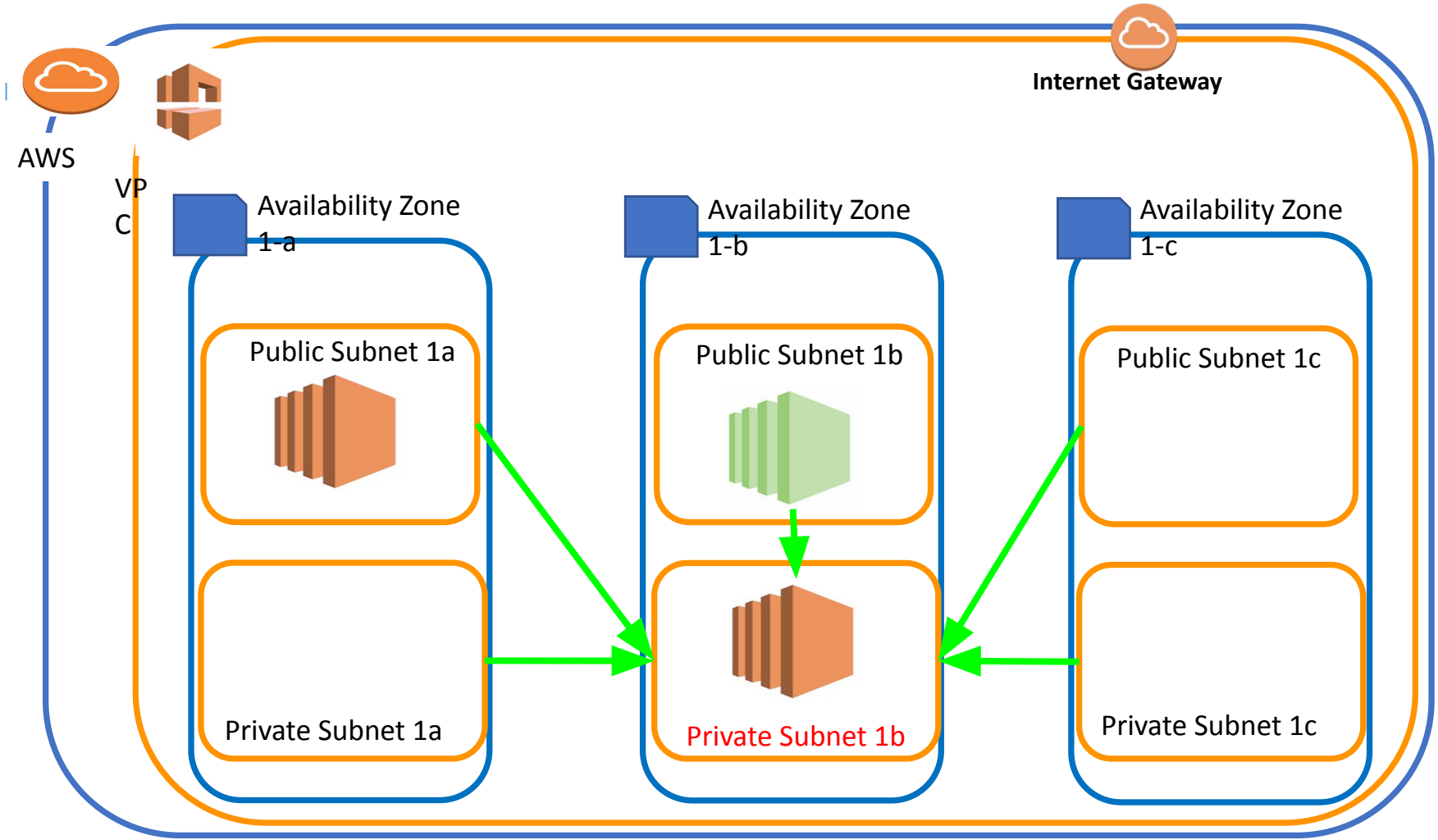
Private Subnets
Internet Connectivity

Public Subnets
Internet Connectivity

VPC-PART-2

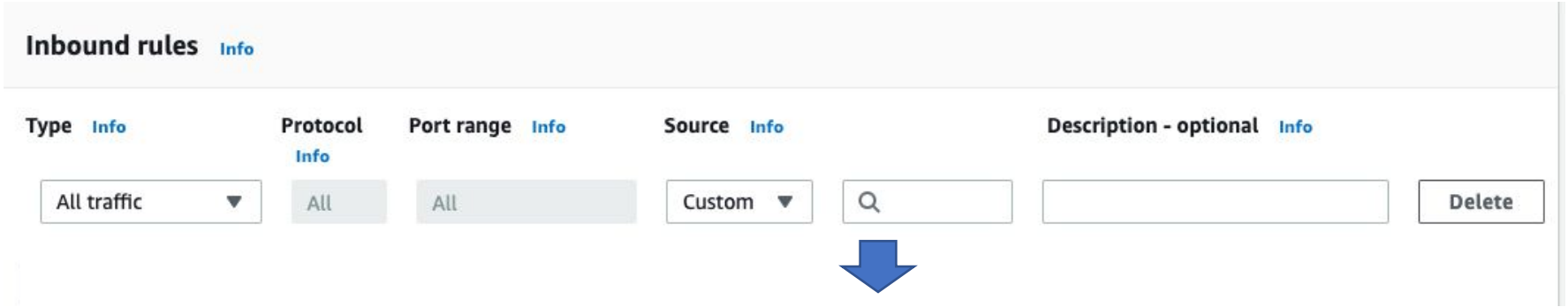
- VPC Solutions
  - Elastic IP
  - Bastion Host /Jump Box
  - NAT Gateway
  - NAT Instance


Public
Subnet
Hello !
Private IP
Private
Subnet


AWS
VP
C
Internet Gateway
Availability Zone
1-a
Availability Zone
1-b
Availability Zone
1-c
Public Subnet 1a
Public Subnet 1b
Public Subnet 1c
Private Subnet 1a
Private Subnet 1b
Private Subnet 1c

Sec. Group Issue

Private Instance Sec.Group



1-Sec. group of Bastion Host –Best practice
2-CIDR Block of “Public Subnet”
3-IP of Bastion Host Instance

AWS

VP
C

Internet Gateway

Availability Zone
1-a

Availability Zone
1-b

Availability Zone
1-c

Public Subnet 1a

Public sg

Public Subnet 1b

Public sg

Public Subnet 1c

Private Subnet 1a

Private Subnet 1b

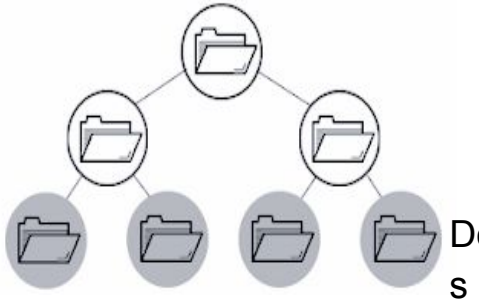
Private sec grp

Private Subnet 1c

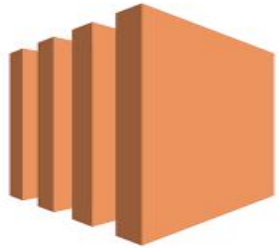
TWO KEYS CREATED FOR SHH AFTER LAUNCHING

PRIVATE KEY

PUBLIC KEY



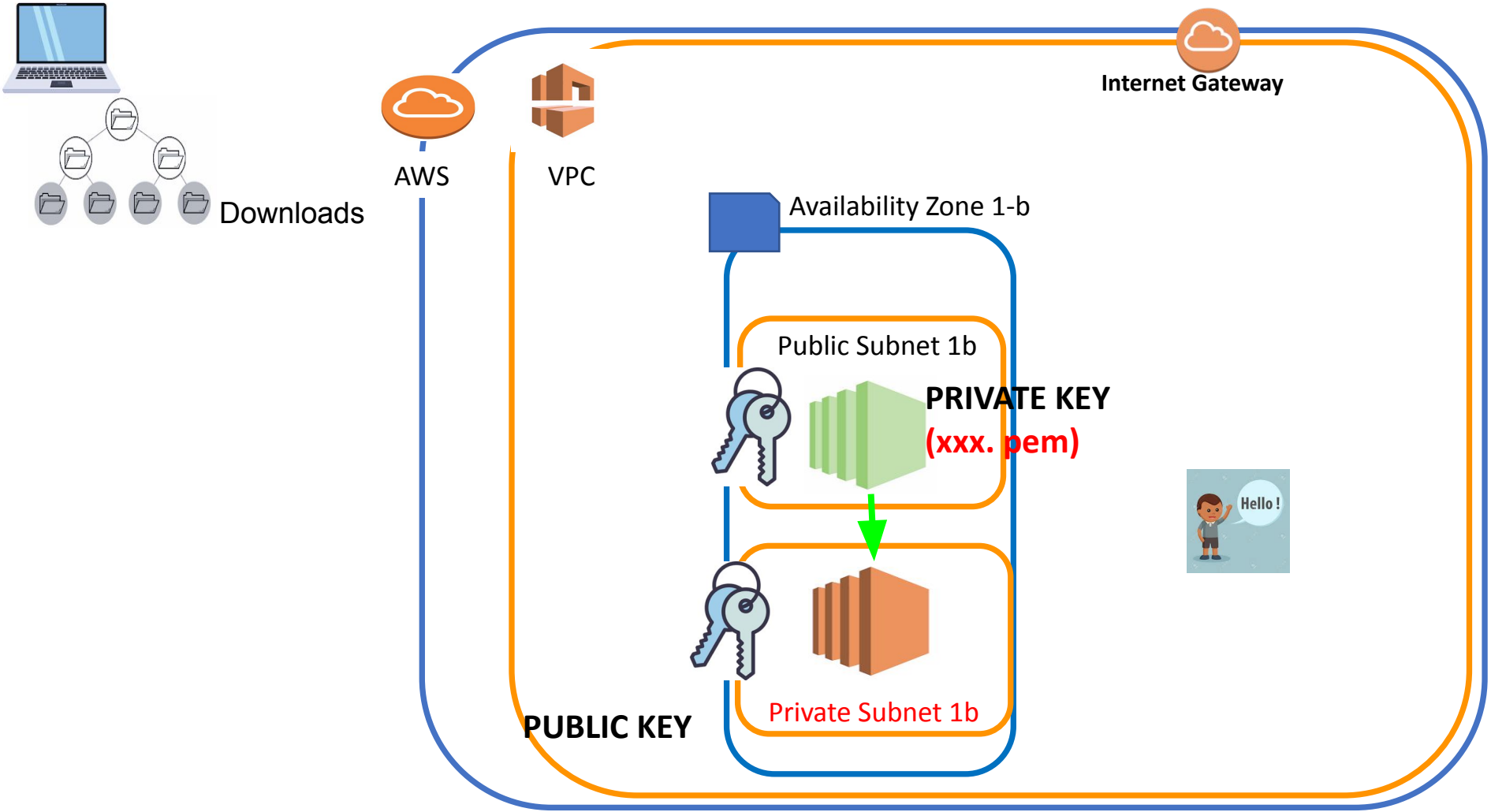
SSH



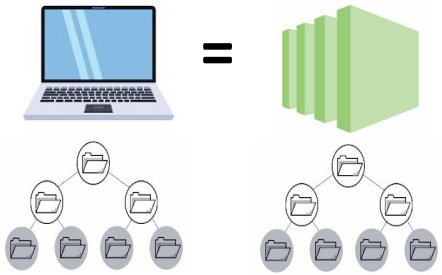
Download
s

PRIVATE KEY
(xxx. pem)

PUBLIC KEY


Downloads
AWS
VPC
Internet Gateway
Availability Zone 1-b
Public Subnet 1b
PRIVATE KEY
(xxx. pem)
Hello !
Private Subnet 1b
PUBLIC KEY

.pem issue



Key.pe
m

Bastion Host-2

Bastion Host-1

Public Subnet 1a

Key.pe

Public Subnet 1c

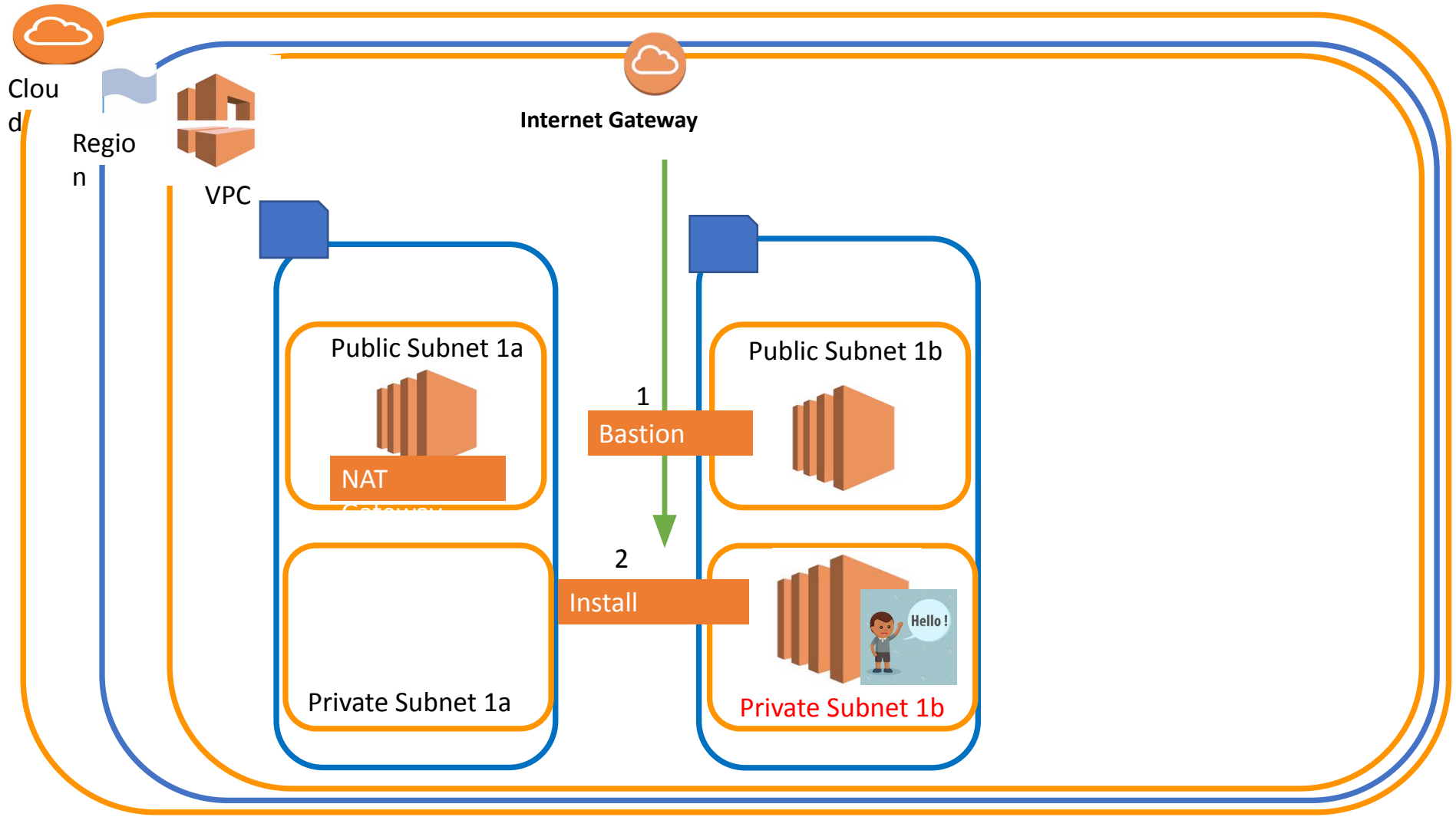
PUBLIC KEY

Private Subnet 1a

PUBLIC KEY

Private Subnet 1c

Key.pem
(PRİVATE KEY)


Cloud
Region
VPC
Internet Gateway
Public Subnet 1a
NAT
Public Subnet 1b
1
Bastion
2
Install
Private Subnet 1a
Hello !
Private Subnet 1b

NAT Gateway

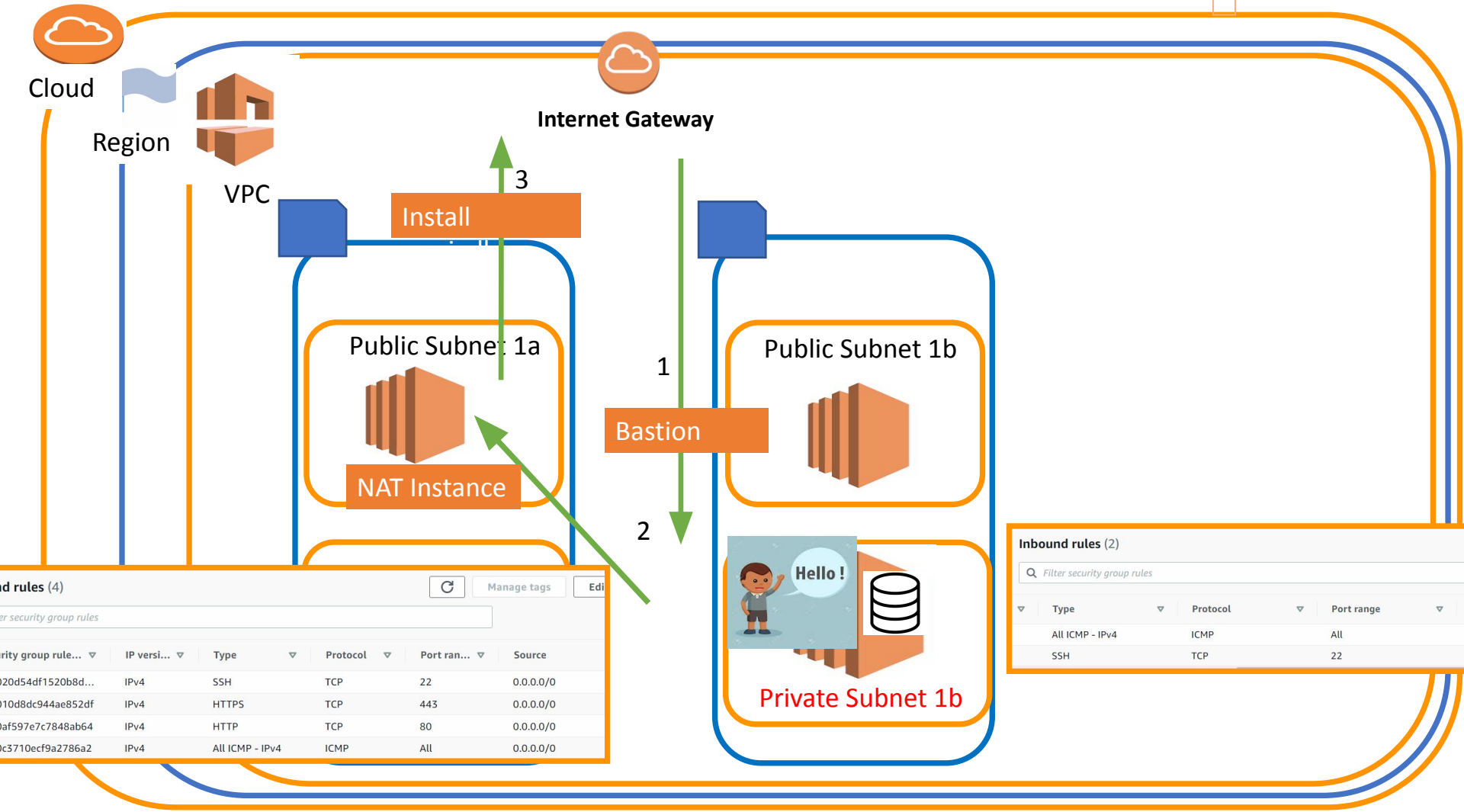
Edit routes

Destination	Target	Status
10.7.0.0/16	local	active
0.0.0.0/0	nat-0ded7d8a9439d336d	active
172.31.0.0/16	pcx-0ecbf98754b602517	active
0.0.0.0/0	igw-0416e7d5a8d836388	

Add route

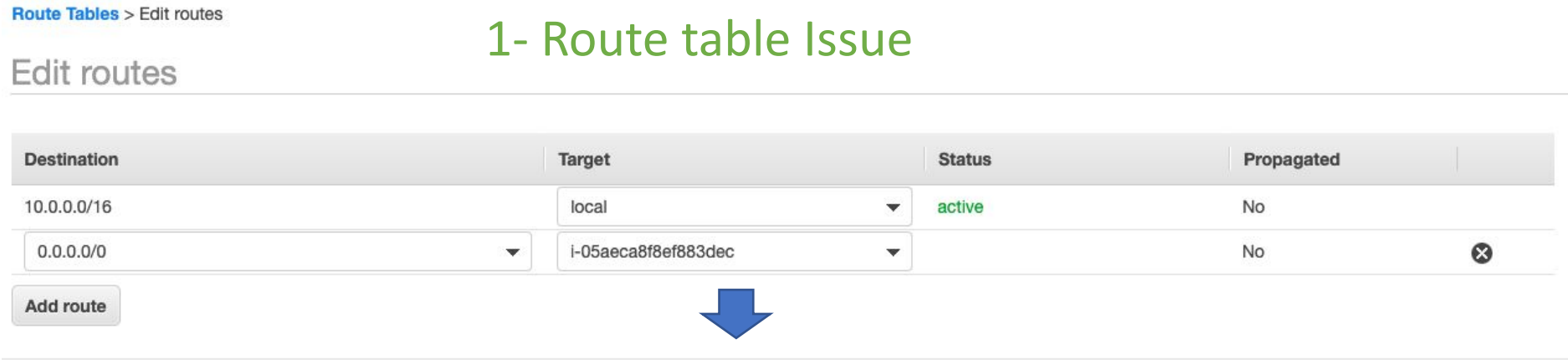
* Required

Route Tables


Cloud
Region
VPC
Internet Gateway
3
Install
Public Subnet 1a
NAT Instance
1
Bastion
2
Public Subnet 1b
Hello !
Private Subnet 1b
d rules (4)
Manage tags
Edi
er security group rules
rity group rule...
IP versi...
Type
Protocol
Port ran...
Source
20d54df1520b8d...
IPv4
SSH
TCP
22
0.0.0.0/0
010d8dc944ae852df
IPv4
HTTPS
TCP
443
0.0.0.0/0
af597e7c7848ab64
IPv4
HTTP
TCP
80
0.0.0.0/0
c3710ecf9a2786a2
IPv4
All ICMP - IPv4
ICMP
All
0.0.0.0/0
Inbound rules (2)
Filter security group rules
Type
Protocol
Port range
All ICMP - IPv4
ICMP
All
SSH
TCP
22

Nat Instance

1- Route table Issue



- Nat Instance

2- Change Source/ Destination Check

- Disable

Local

NAT Instance

Edit routes

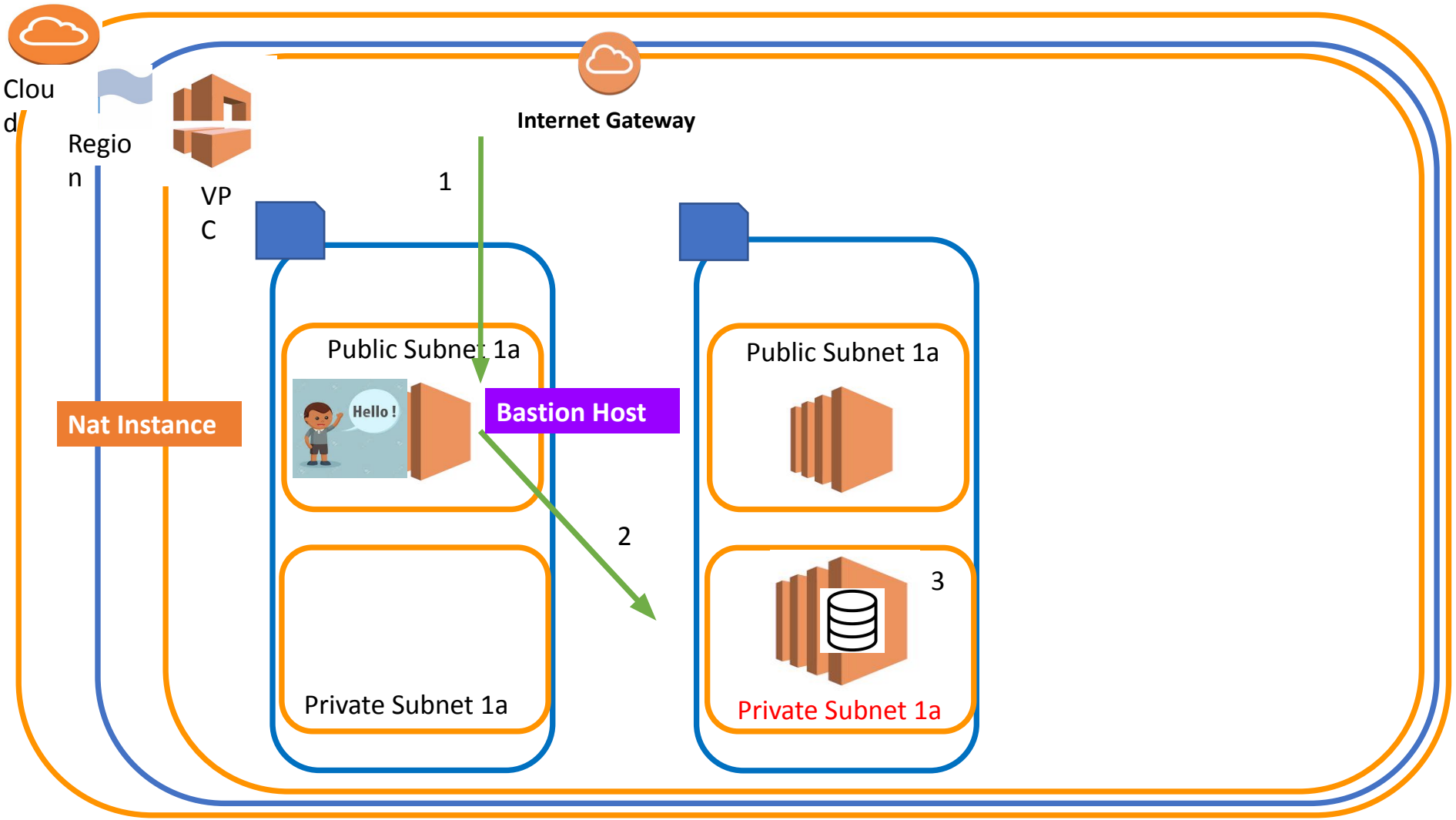
Destination	Target	Status
10.7.0.0/16	local	active
0.0.0.0/0	nat-0ded7d8a9439d336d	active
172.31.0.0/16	pcx-0ecbf98754b602517	active
0.0.0.0/0	igw-0416e7d5a8d836388	

Add route

* Required

Route Tables

NAT Gateway


Clou
d
Regio
n
VP
C
Internet Gateway
1
Public Subnet 1a
Hello !
Bastion Host
Nat Instance
2
Private Subnet 1a
Public Subnet 1a
3
Private Subnet 1a

AWS

VP
C

Internet Gateway

Availability Zone
1-a

Availability Zone
1-b

Availability Zone
1-c

Public Subnet 1a

Public Subnet 1b

Public Subnet 1c

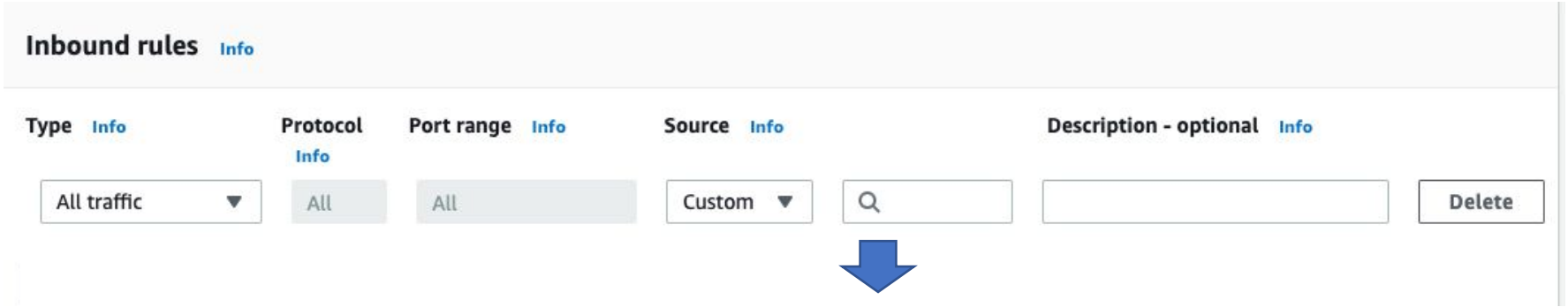
Private Subnet 1a

Private Subnet 1b

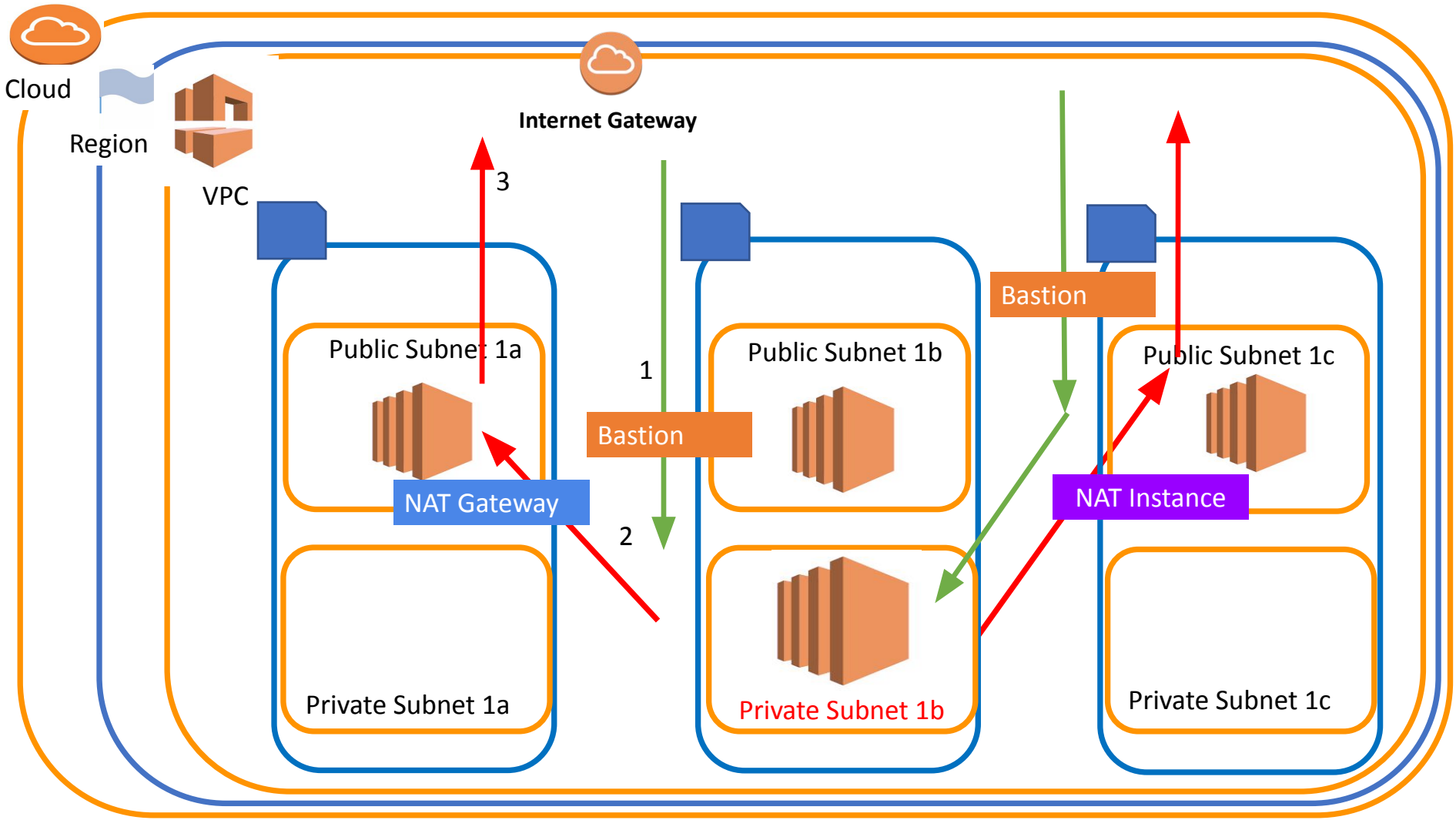
Private Subnet 1c

Sec. Group Issue

Private Instance Sec.Group



1-Sec. group of Nat Instace


Cloud
Region
VPC
Internet Gateway
3
1
2
Public Subnet 1a
Public Subnet 1b
Public Subnet 1c
Bastion
Bastion
NAT Gateway
NAT Instance
Private Subnet 1a
Private Subnet 1b
Private Subnet 1c

Conclusion

Nat gateway-Nat instance

Change Route table of Private Subnet

Helps Private instance to install software package*

Nat instance/Gateway = Unique instance

Bastion Host

Change Sec. Group

Helps Public Instance to connect Private instance

Bastion Host = Ordinary Instance in public Subnet

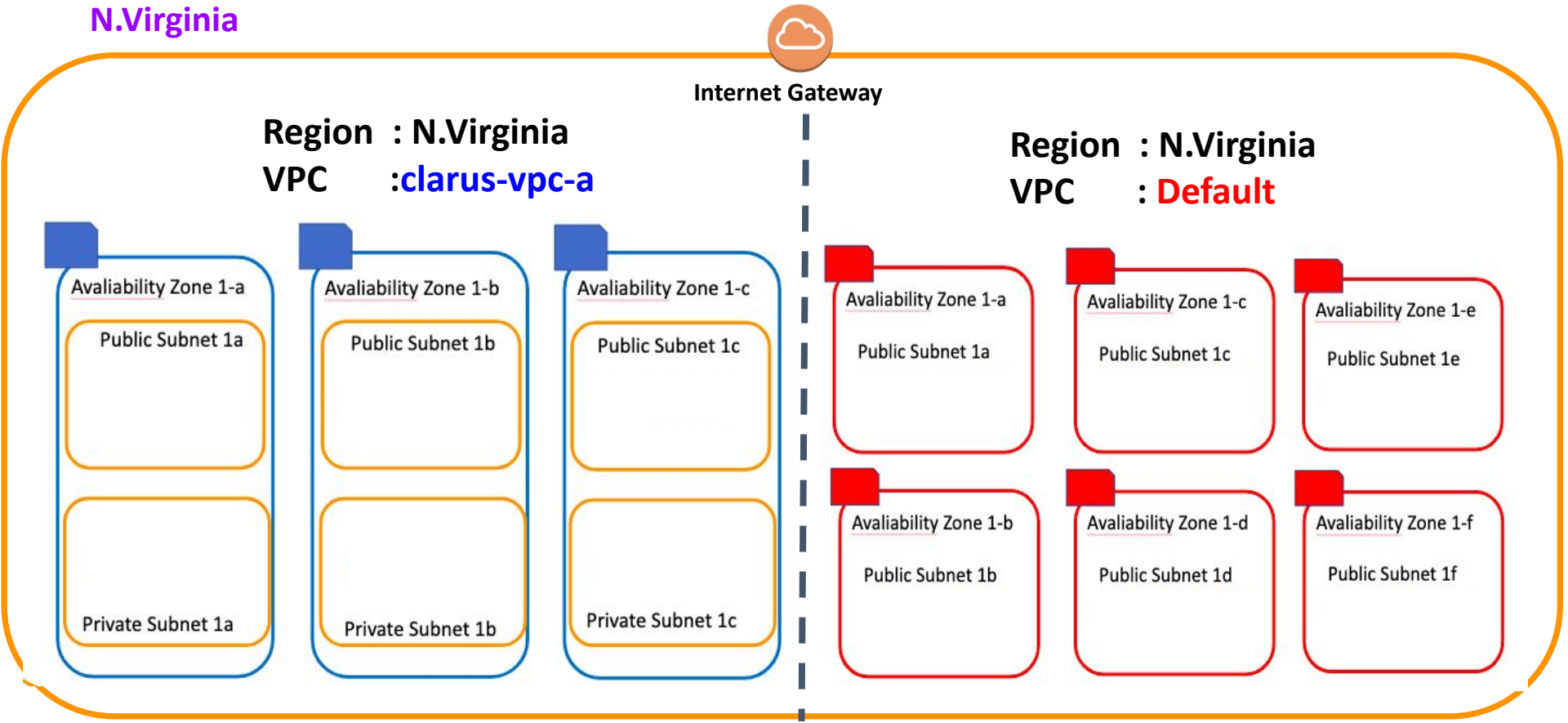
*Sec grup : Must be SSH, HTTP >>>>0.0.0.0/0

	NAT Gateway	NAT Instance
Managed	Managed by AWS	Managed by you
Availability	Highly available within an AZ	Not highly available (would require scripting)
Bandwidth	Up to 45 Gbps	Depends on the bandwidth of the EC2 instance type selected
Maintenance	Managed by AWS	Managed by you
Performance	Optimized for NAT	Amazon Linux AMI configured to perform NAT
Public IP	Elastic IP that cannot be detached	Elastic IP that can be detached
Security Groups	Cannot associate with a Security Group	Can associate with a Security Group
Bastion Host	Not supported	Can be used as a bastion host

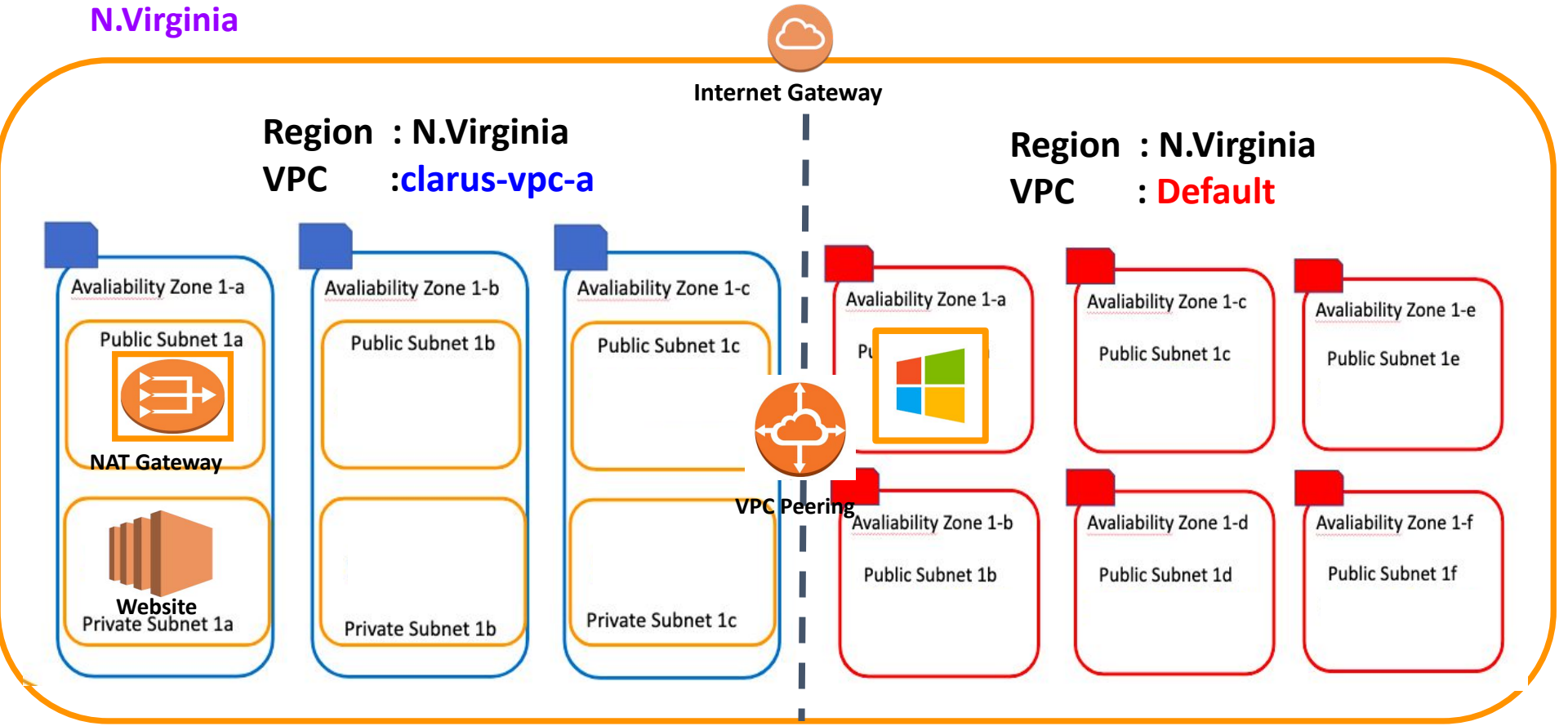
VPC-PART-3

- VPC Endpoint
- VPC Peering
- VPN & Direct Connect

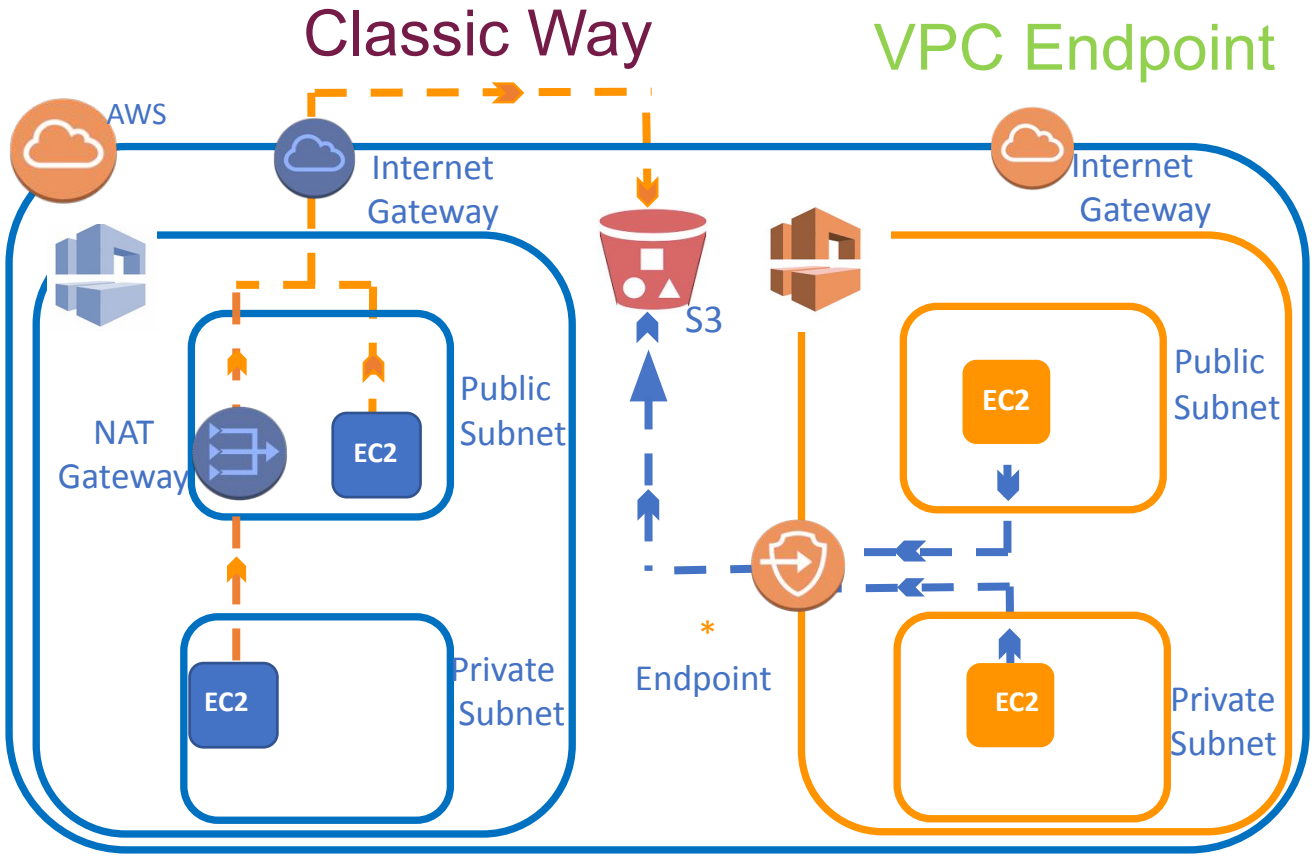
N.Virginia

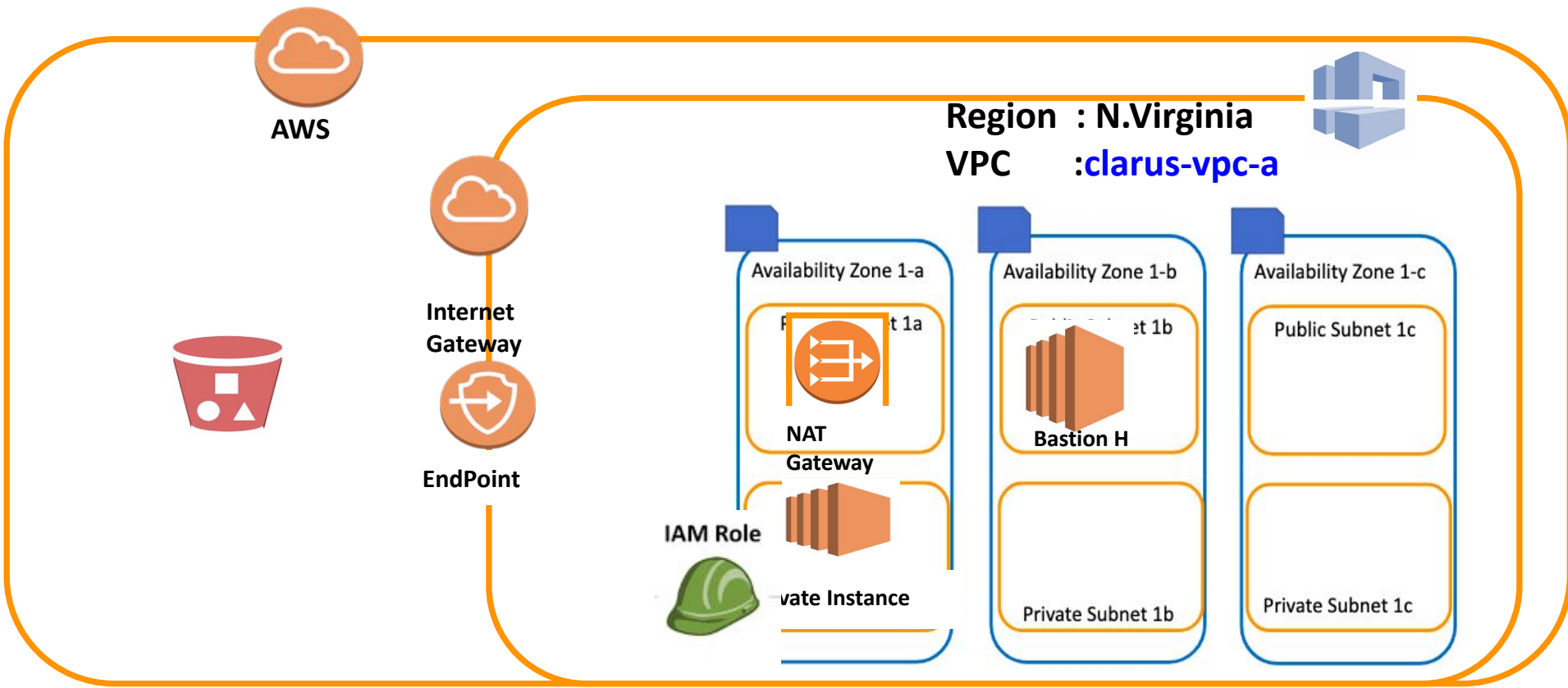

Internet Gateway
Region : N.Virginia
VPC :clarus-vpc-a
Avaliability Zone 1-a
Public Subnet 1a
Private Subnet 1a
Avaliability Zone 1-b
Public Subnet 1b
Private Subnet 1b
Avaliability Zone 1-c
Public Subnet 1c
Private Subnet 1c
Region : N.Virginia
VPC : Default
Avaliability Zone 1-a
Public Subnet 1a
Avaliability Zone 1-c
Public Subnet 1c
Avaliability Zone 1-e
Public Subnet 1e
Avaliability Zone 1-b
Public Subnet 1b
Avaliability Zone 1-d
Public Subnet 1d
Avaliability Zone 1-f
Public Subnet 1f

N.Virginia


Internet Gateway
Region : N.Virginia
VPC :clarus-vpc-a
Region : N.Virginia
VPC : Default
Avaliability Zone 1-a
Public Subnet 1a
NAT Gateway
Website
Private Subnet 1a
Avaliability Zone 1-b
Public Subnet 1b
Private Subnet 1b
Avaliability Zone 1-c
Public Subnet 1c
Private Subnet 1c
VPC Peering
Avaliability Zone 1-a
Avaliability Zone 1-b
Public Subnet 1b
Avaliability Zone 1-c
Public Subnet 1c
Avaliability Zone 1-d
Public Subnet 1d
Avaliability Zone 1-e
Public Subnet 1e
Avaliability Zone 1-f
Public Subnet 1f

VPC Endpoint




AWS
Region : N.Virginia
VPC :clarus-vpc-a
Internet Gateway
EndPoint
Availability Zone 1-a
Availability Zone 1-b
Availability Zone 1-c
NAT Gateway
Bastion H
Public Subnet 1c
IAM Role
Private Subnet 1b
Private Subnet 1c

	Interface Endpoint	Gateway Endpoint
What	Elastic Network Interface with a Private IP	A gateway that is a target for a specific route
How	Uses DNS entries to redirect traffic	Uses prefix lists in the route table to redirect traffic
Which services	API Gateway, CloudFormation, CloudWatch etc.	Amazon S3, DynamoDB
Security	Security Groups	VPC Endpoint Policies

VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by AWS **PrivateLink** without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection

PrivateLink is a technology that enables you to **privately access services by using private IP addresses.**

There are two different types of VPC endpoint:

An interface endpoint is an elastic network interface with a private IP address from the IP address range of your subnet. **It serves as an entry point for traffic destined to a supported AWS service or a VPC endpoint service.** Interface endpoints are powered by AWS PrivateLink

Instances in your VPC do not require public IP addresses to communicate with resources in the service. Traffic between your VPC and the other service does not leave the Amazon network.

With a **gateway endpoint** you configure your route table to point to the endpoint. Amazon S3 and DynamoDB use gateway endpoints.

VPC-PART-4

- WORDPRESS WITH LAMP STACK ON VPC
- NACL TABLES