ondia

Amazon VPC-4

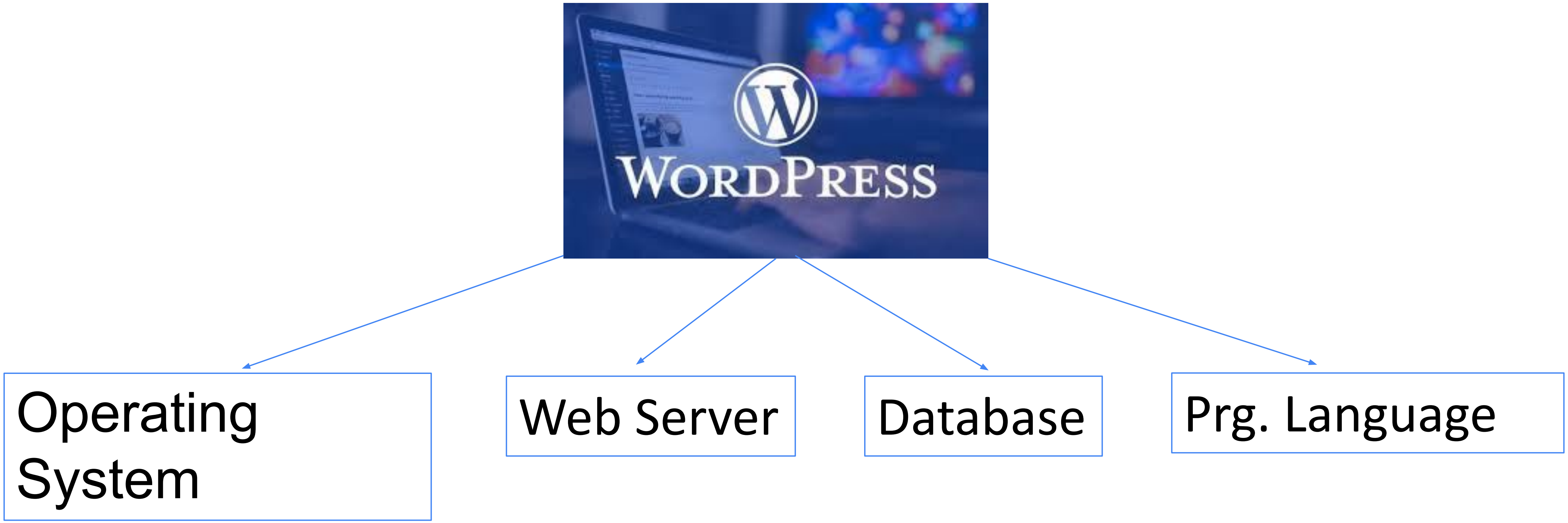
AGENDA

- WORDPRESS WITH LAMP STACK ON VPC
- NACL TABLES

WORDPRESS WITH LAMP STACK ON VPC

Dynamic Website

Dynamic Website



Operating System

Web Server

Database

Prg. Language

Setup Wordpress with Database

LAMP:
Linux
Apache
MySQL
MySQL
php
PHP

Operating System

Web Server

Database

Progr. language

User Data

✓

Installed-ready

LAMP:

Linux
Apache
MySQL
MySQL
php
PHP

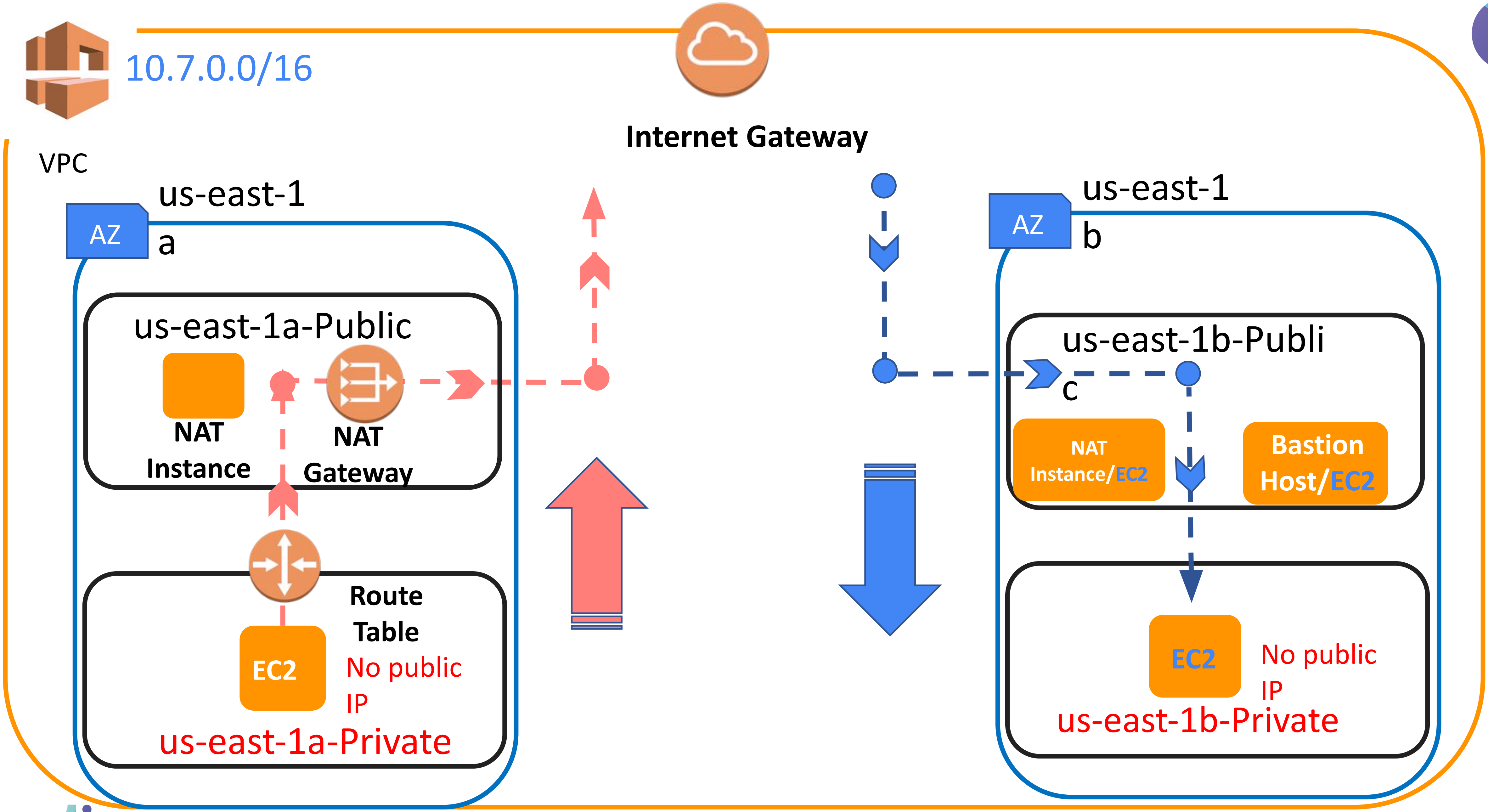
EC2 Amazon Linux 2023 ✓

User Data ✓

User Data ✓

User Data ✓

User Data ✓


10.7.0.0/16
VPC
Internet Gateway
AZ
us-east-1
a
us-east-1a-Public
NAT
Instance
NAT
Gateway
Route
Table
EC2
No public
IP
us-east-1a-Private
AZ
us-east-1
b
us-east-1b-Publi
c
NAT
Instance/EC2
Bastion
Host/EC2
EC2
No public
IP
us-east-1b-Private

Operating System

Web Server

Database

Progr. language

User Data

LAMP: ✓

Installed-ready

MySQL
Linux
Apache
MySQL
php
PHP

EC2 Amazon Linux 2 ✓

User Data ✓

?

V

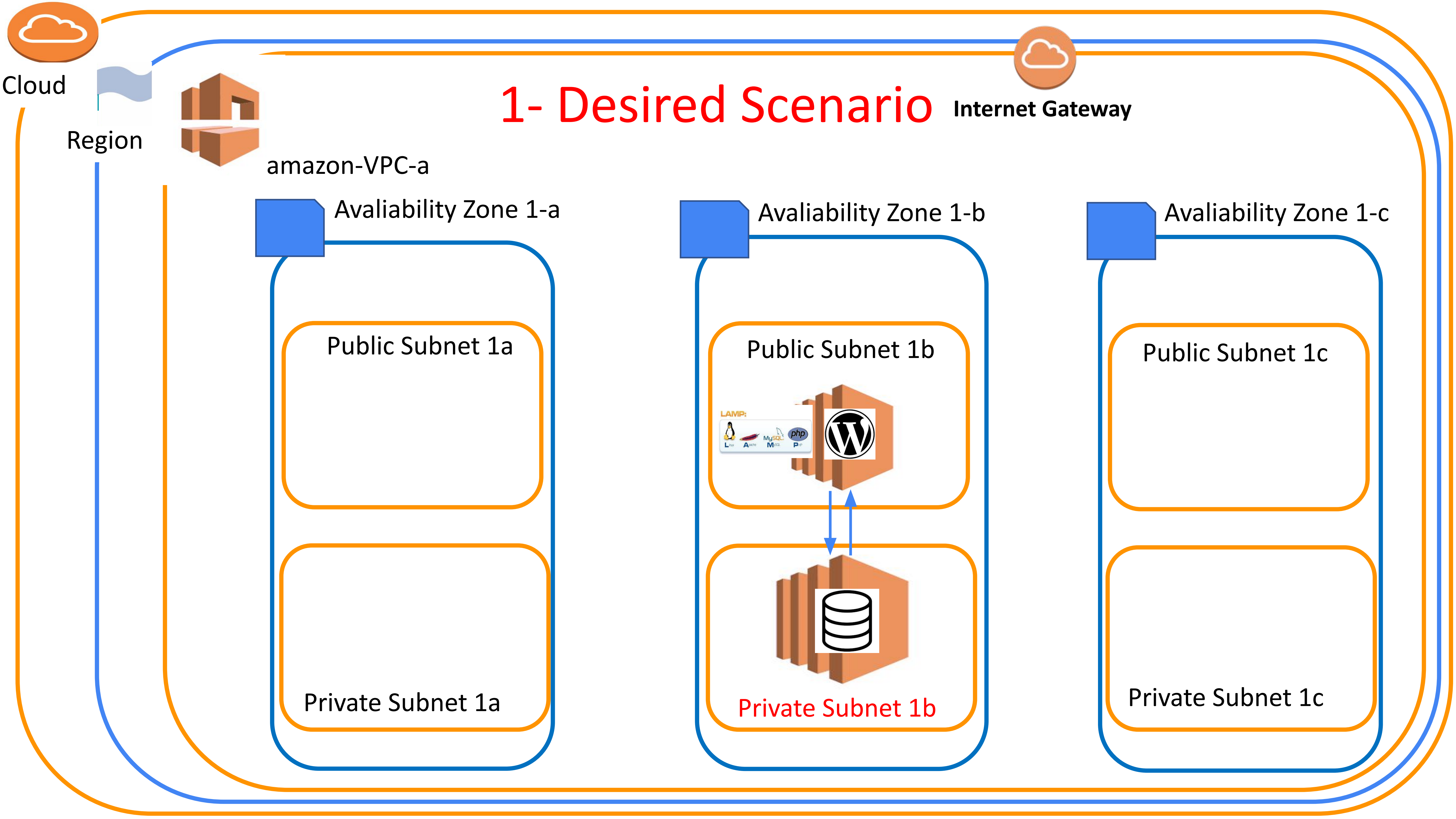
V

User Data ✓

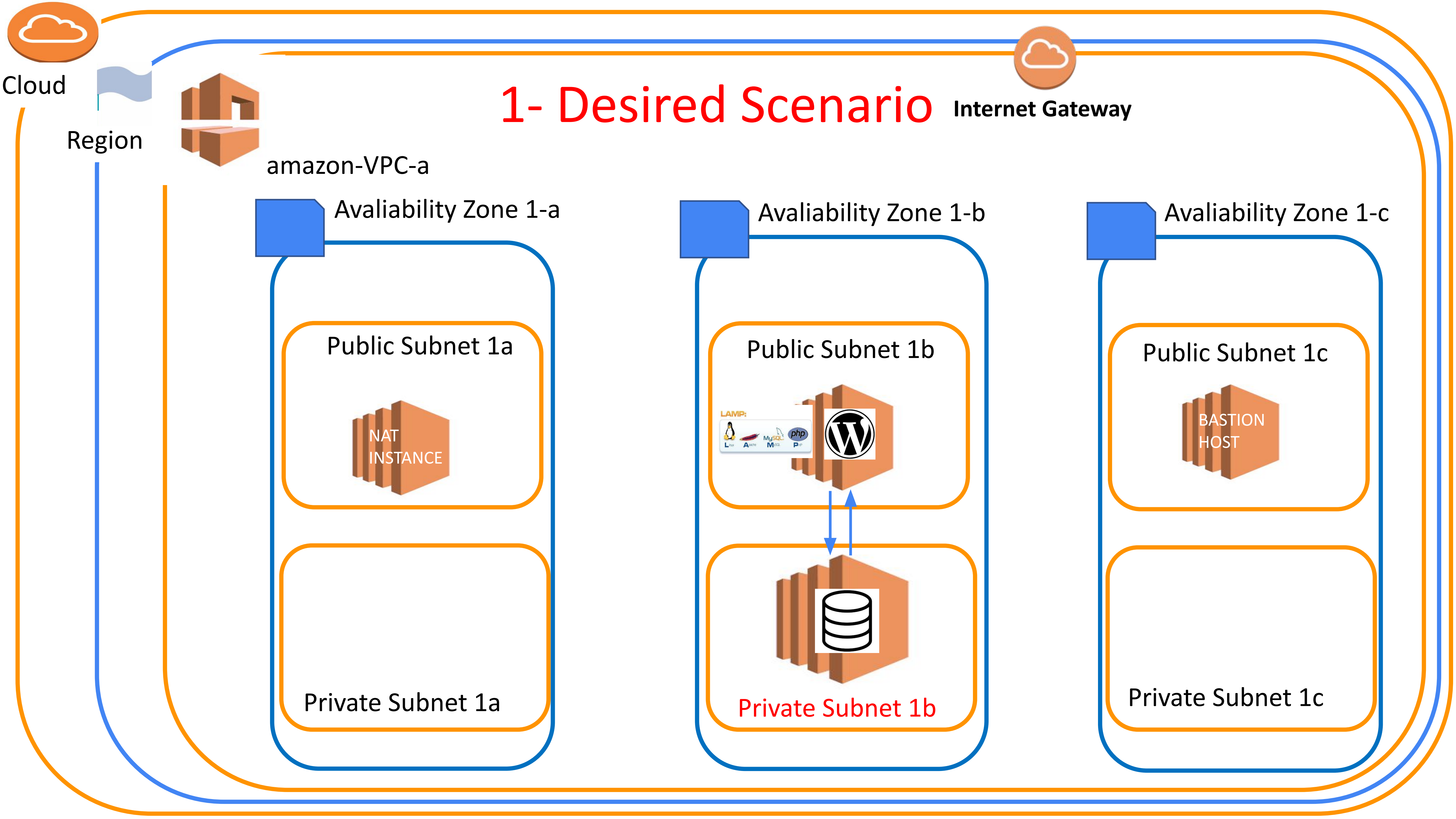
User Data ✓

It is in another instance in the Private Subnet

1- Desired Scenario



1- Desired Scenario



Cloud

Region

amazon-VPC-a

Internet Gateway

Avaliability Zone 1-a

Public Subnet 1a

NAT INSTANCE

Private Subnet 1a

Avaliability Zone 1-b

Public Subnet 1b

Private Subnet 1b

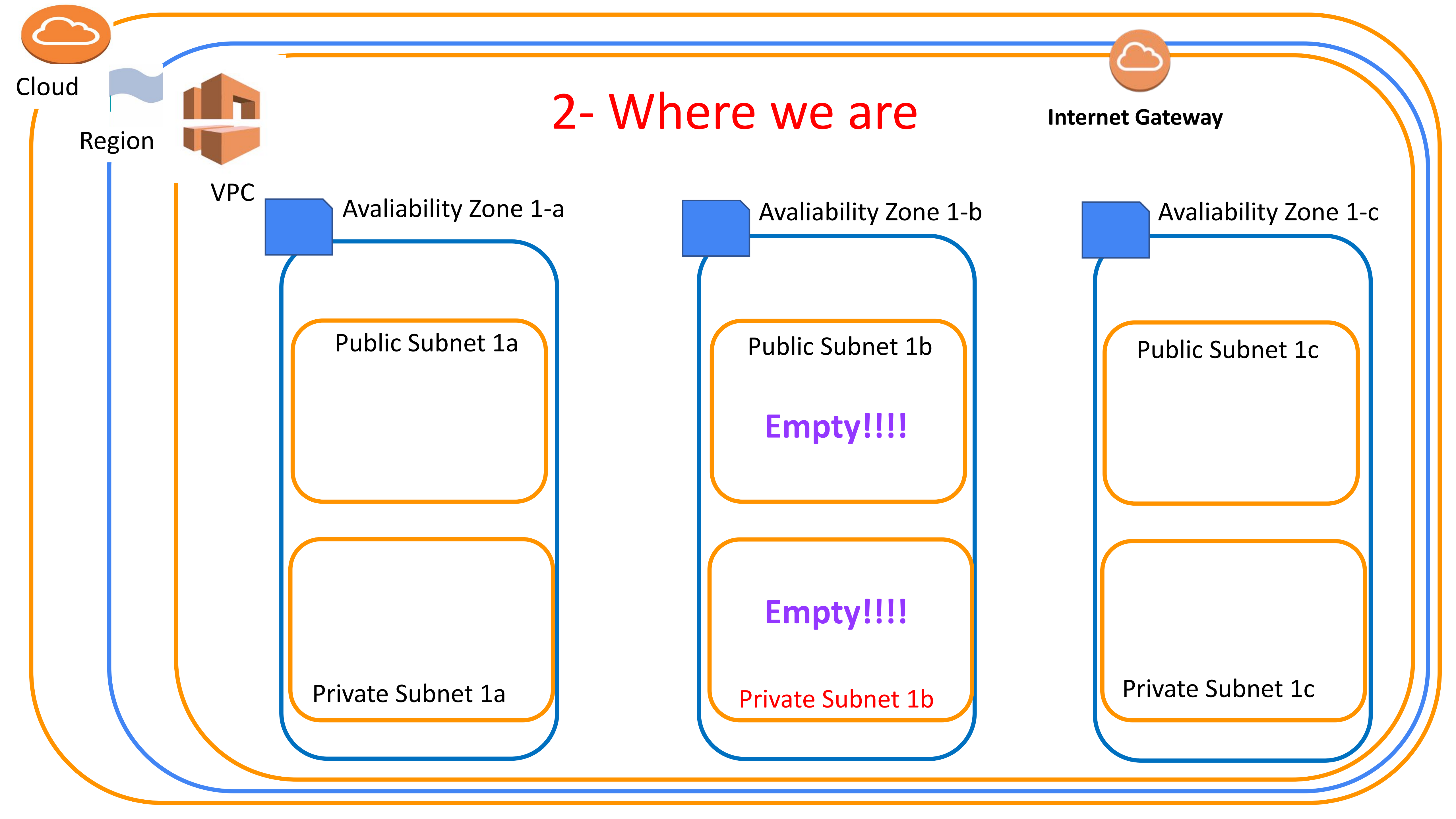
Avaliability Zone 1-c

Public Subnet 1c

BASTION HOST

Private Subnet 1c

2- Where we are



Cloud

Region

VPC

Internet Gateway

Avaliability Zone 1-a

Public Subnet 1a

Private Subnet 1a

Avaliability Zone 1-b

Public Subnet 1b

Empty!!!!

Empty!!!!

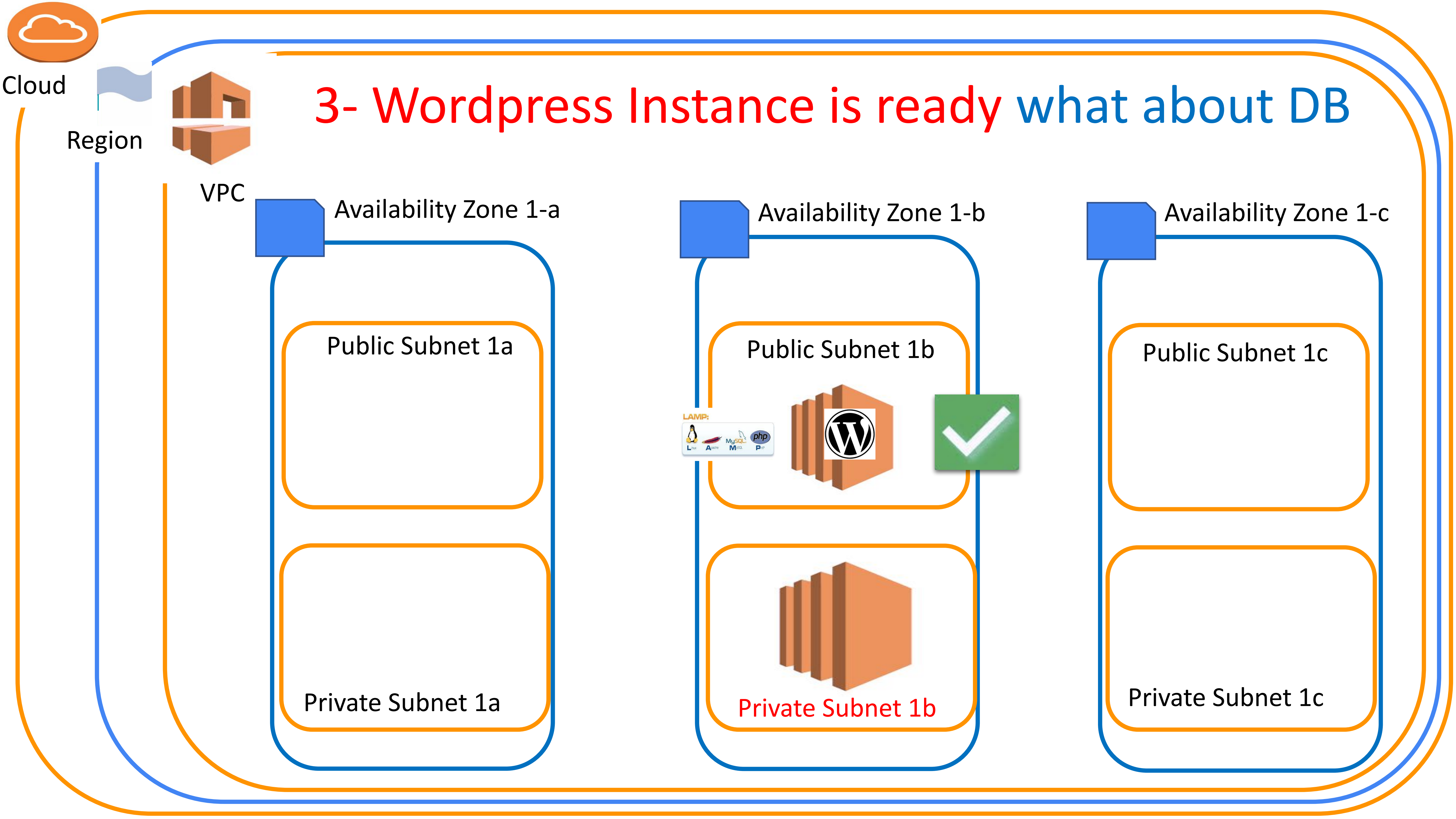
Private Subnet 1b

Avaliability Zone 1-c

Public Subnet 1c

Private Subnet 1c

3- Wordpress Instance is ready what about DB



Cloud

Region

VPC

Availability Zone 1-a

Public Subnet 1a

Private Subnet 1a

Availability Zone 1-b

Public Subnet 1b

Private Subnet 1b

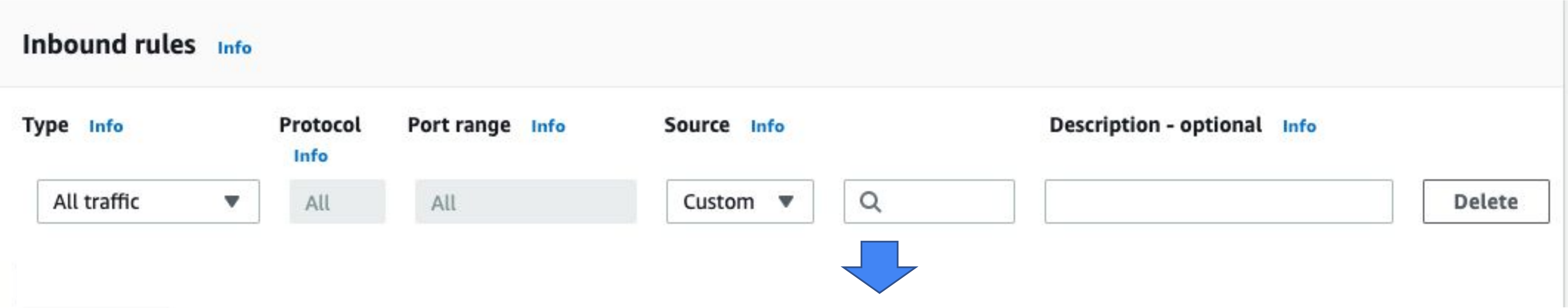
Availability Zone 1-c

Public Subnet 1c

Private Subnet 1c

Security Group Best Practice

Bastion Host



Inbound rules Info

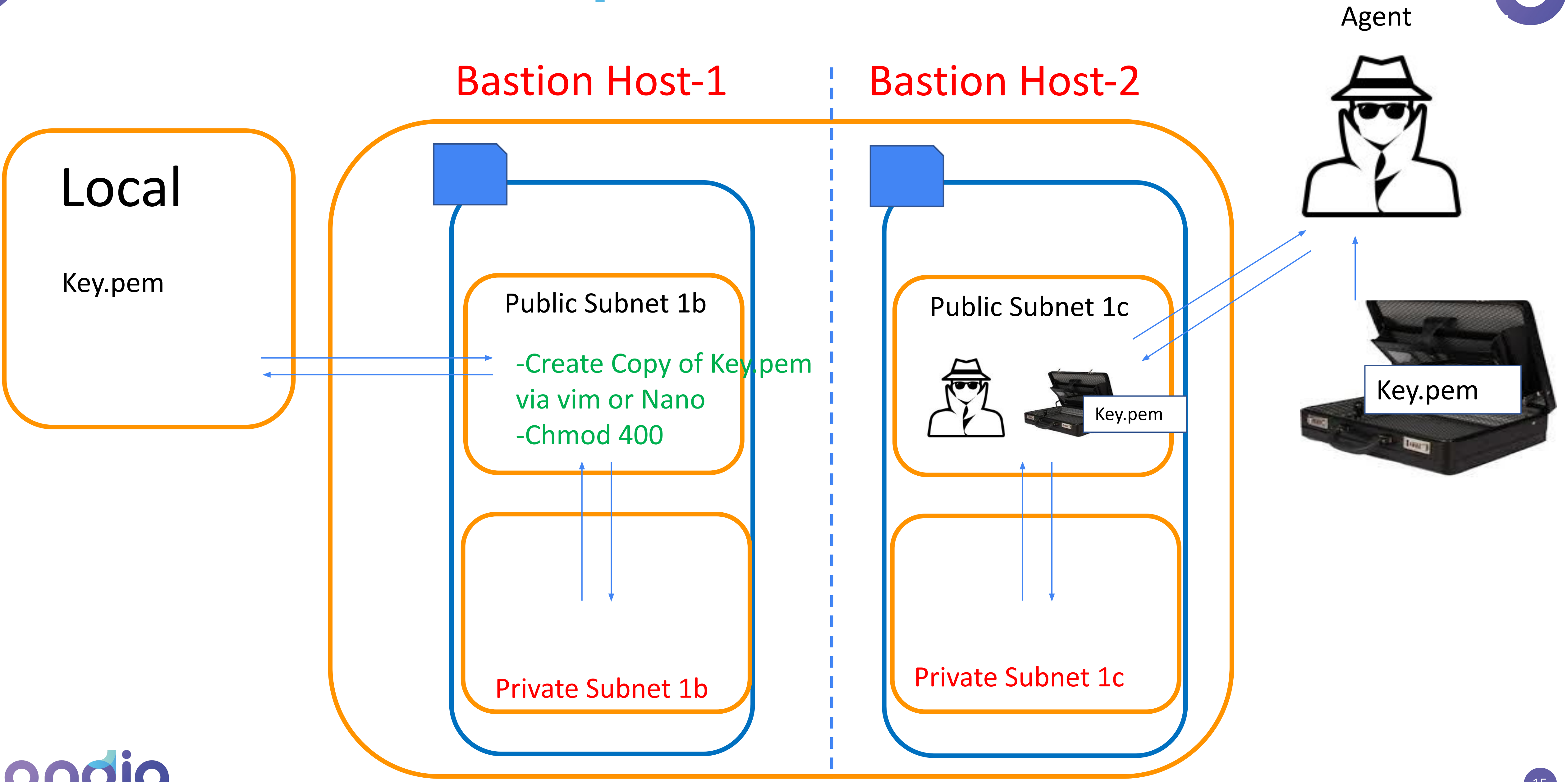
Type Info	Protocol Info	Port range Info	Source Info		Description - optional Info	
All traffic ▼	All	All	Custom ▼	🔍		Delete

1-Sec. group of Bastion Host –Best practice

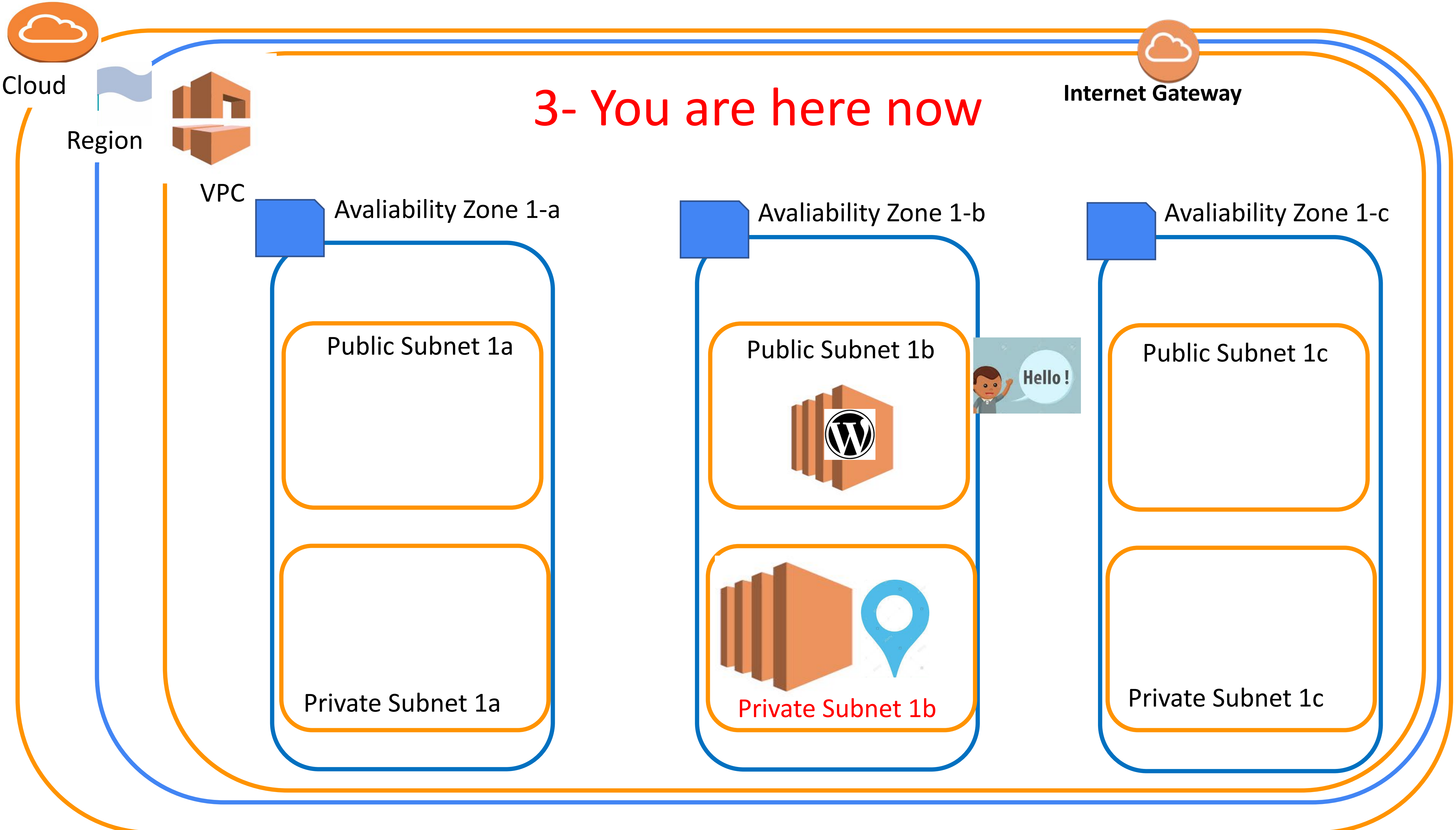
2-CIDR Block of "Public Subnet"

3-IP of Bastion Host Instance

.pem Issue


Bastion Host-1
Bastion Host-2
Agent
Local
Key.pem
Public Subnet 1b
-Create Copy of Key.pem
via vim or Nano
-Chmod 400
Private Subnet 1b
Public Subnet 1c
Key.pem
Private Subnet 1c
Key.pem

3- You are here now



Cloud

Region

VPC

Internet Gateway

Avaliability Zone 1-a

Public Subnet 1a

Private Subnet 1a

Avaliability Zone 1-b

Public Subnet 1b

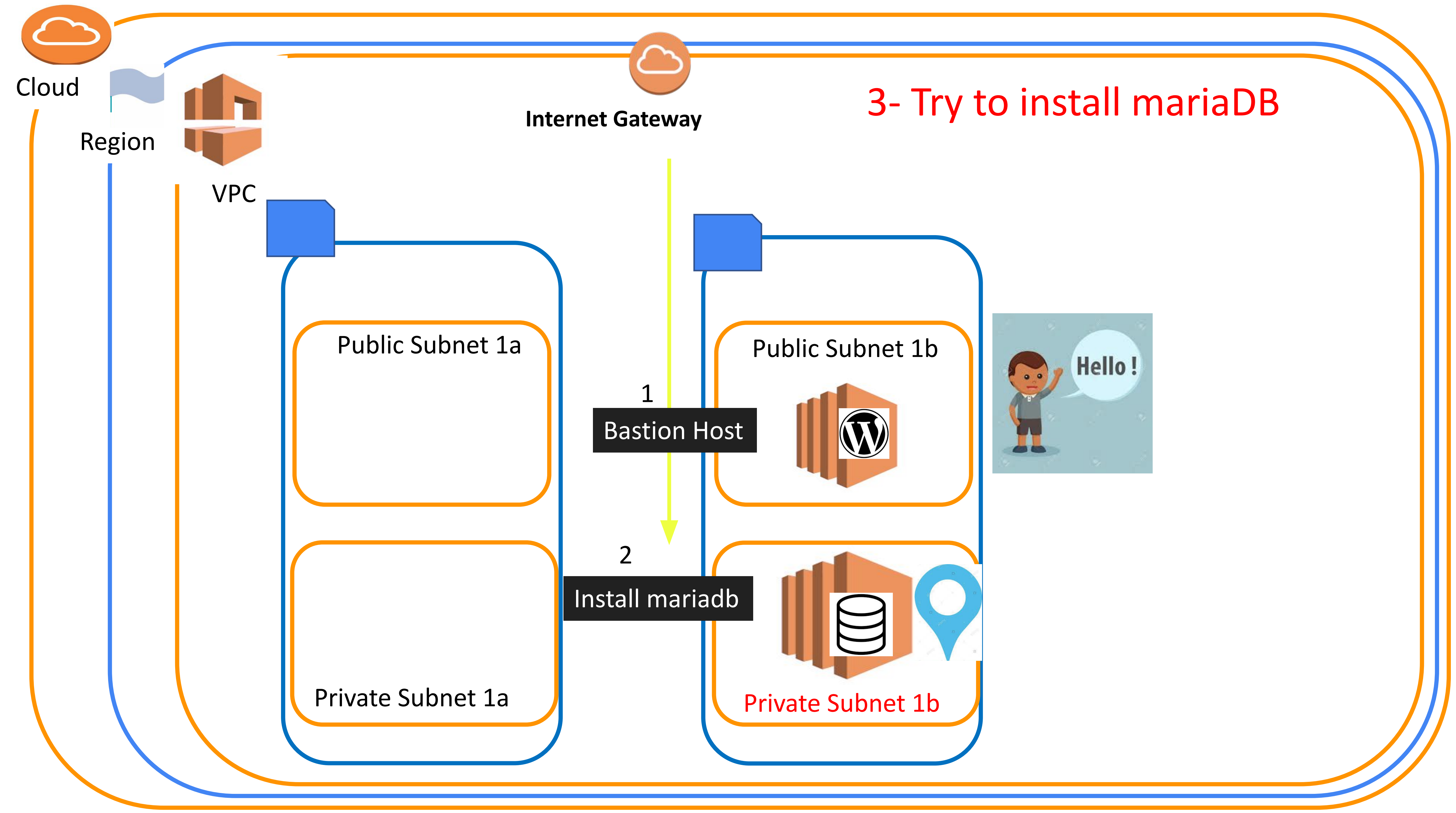
Private Subnet 1b

Avaliability Zone 1-c

Public Subnet 1c

Private Subnet 1c

3- Try to install mariaDB



Cloud

Region

VPC

Internet Gateway

Public Subnet 1a

Private Subnet 1a

1

Bastion Host

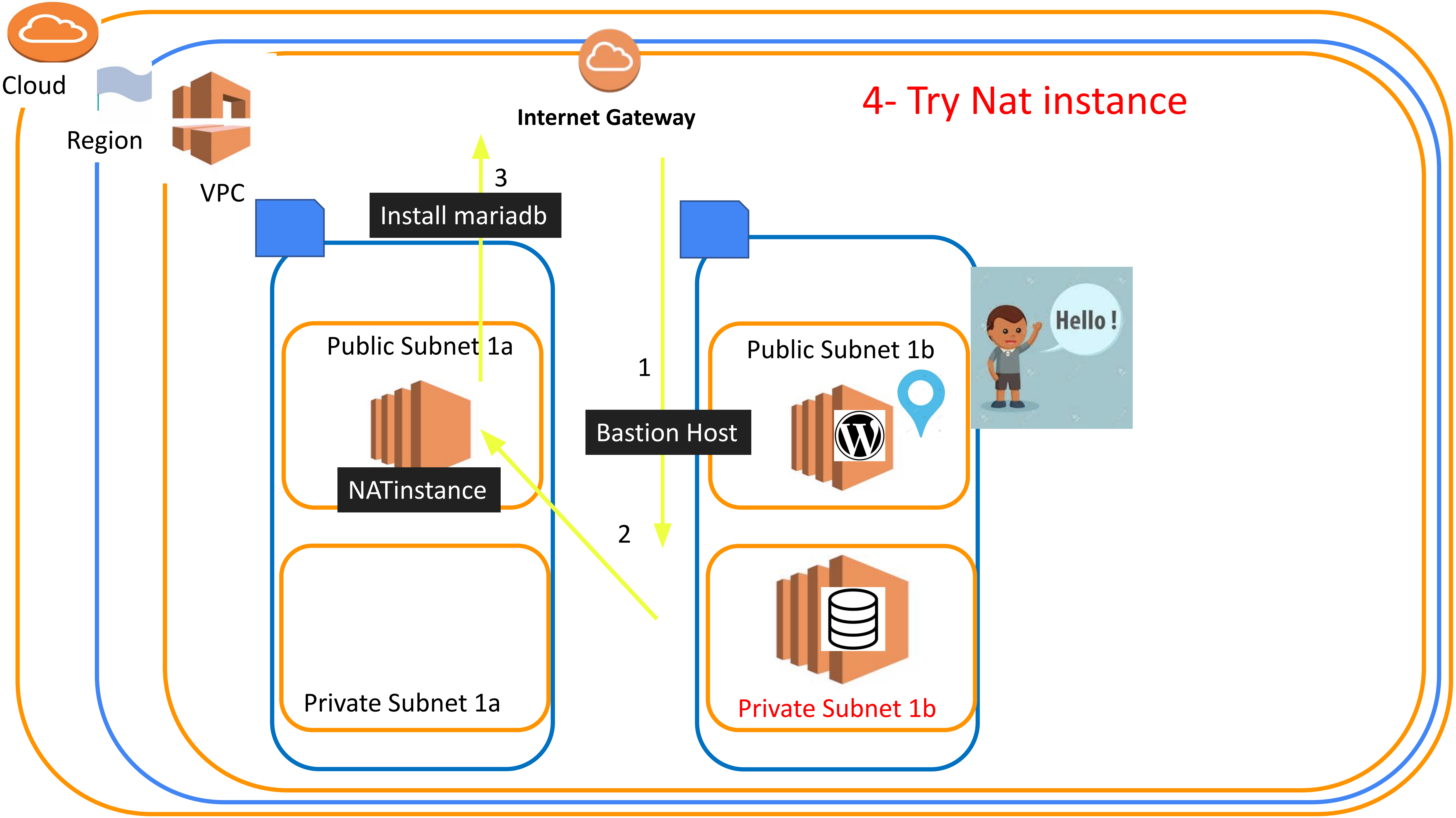
2

Install mariadb

Public Subnet 1b

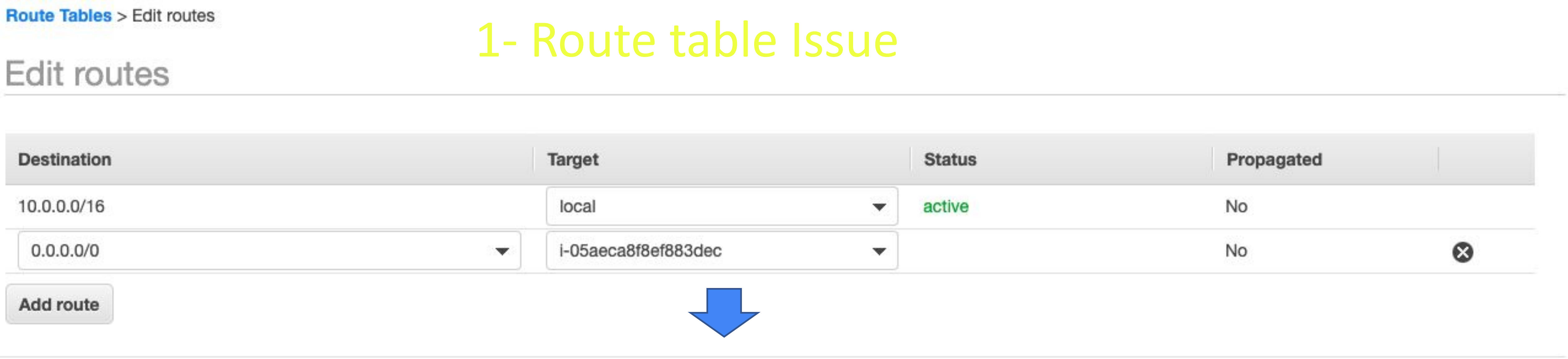
Private Subnet 1b

4- Try Nat instance



NAT INSTANCE

1- Route table Issue



Route Tables > Edit routes

Edit routes

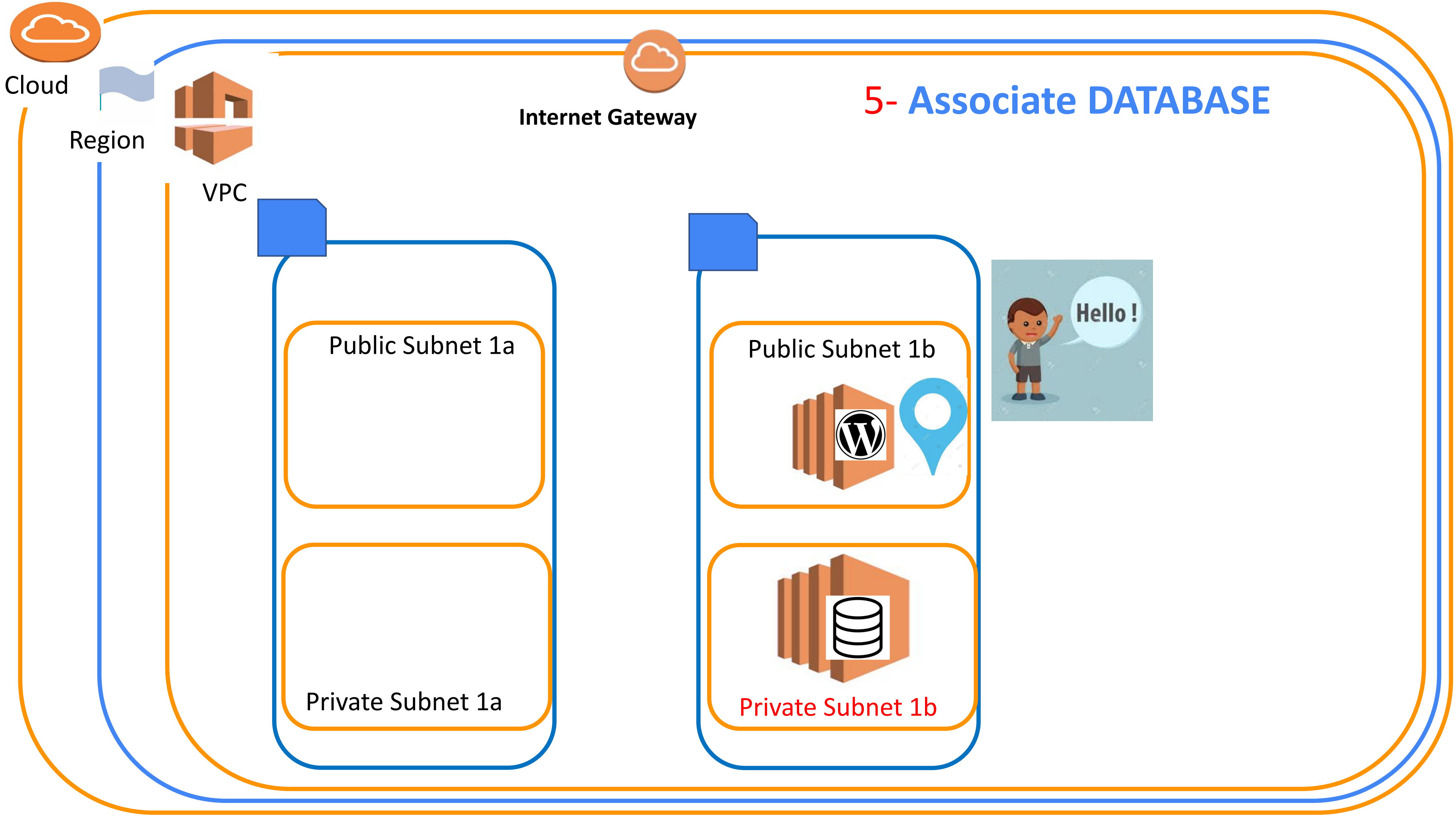
Destination	Target	Status	Propagated	
10.0.0.0/16	local	active	No	
0.0.0.0/0	i-05aeca8f8ef883dec		No	⊗

- Nat instance

2- Change Source/ Destination Check

- Disable

5- Associate DATABASE



Cloud

Region

VPC

Internet Gateway

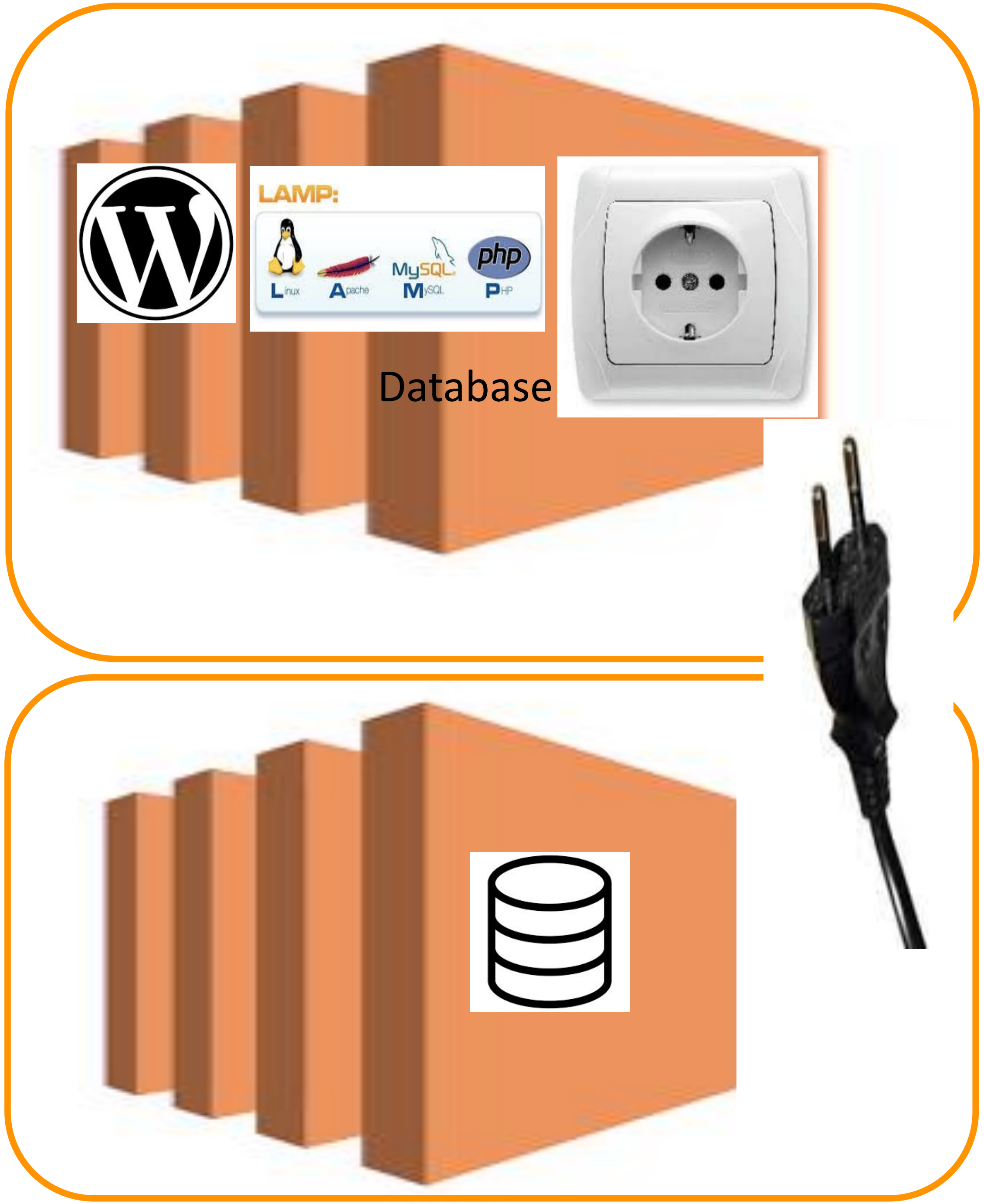
Public Subnet 1a

Private Subnet 1a

Public Subnet 1b

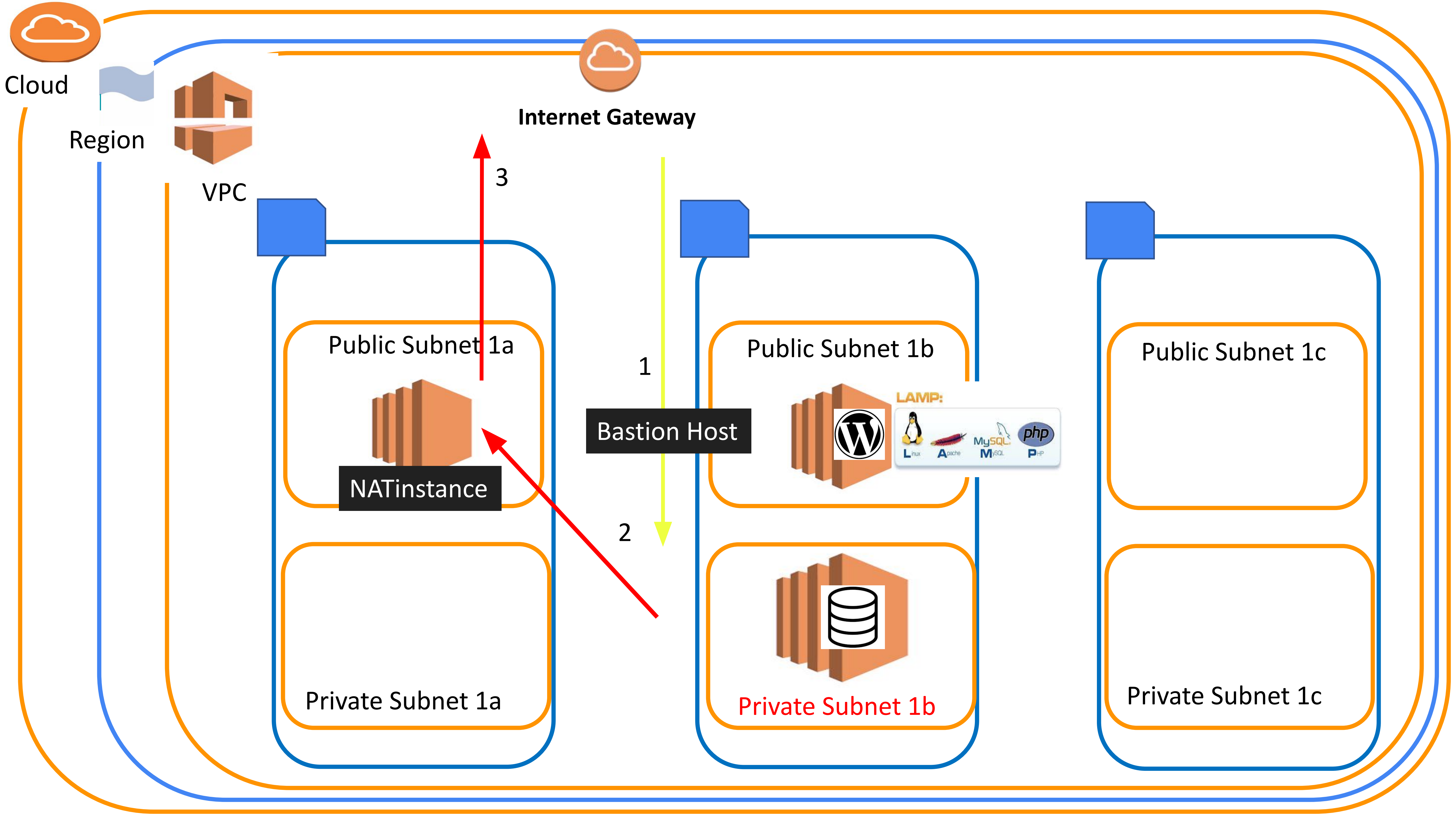
Private Subnet 1b

Associate DATABASE



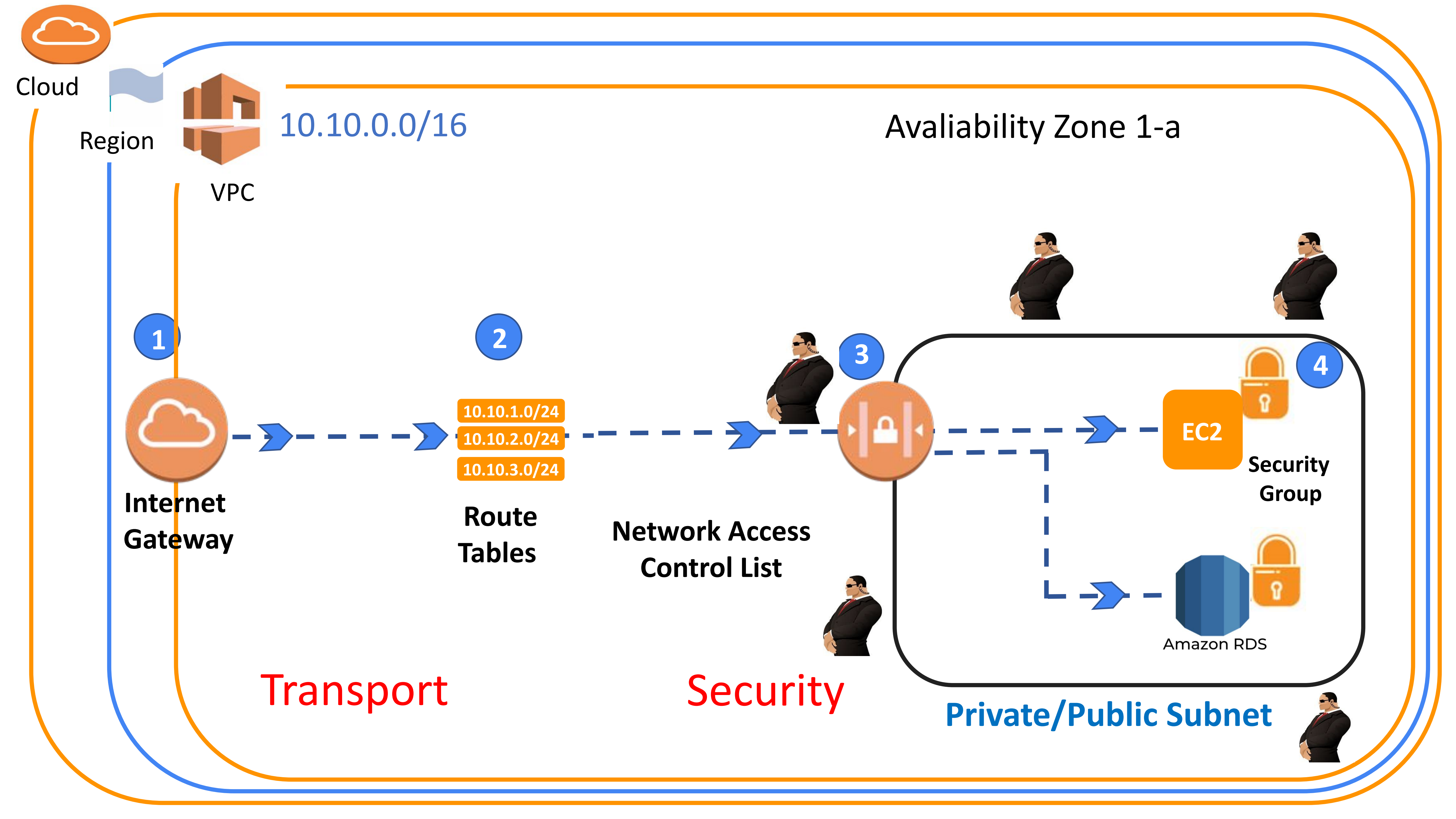
Public Subnet 1b

Private Subnet 1b


Cloud
Region
VPC
Internet Gateway
3
1
2
Public Subnet 1a
NATinstance
Bastion Host
Public Subnet 1b
LAMP:
Linux
Apache
MySQL
PHP
Public Subnet 1c
Private Subnet 1a
Private Subnet 1b
Private Subnet 1c

NACL

(NETWORK ACCESS LISTS)



Cloud

Region

VPC

10.10.0.0/16

Avaliability Zone 1-a

1

Internet Gateway

2

10.10.1.0/24

10.10.2.0/24

10.10.3.0/24

Route Tables

3

Network Access Control List

4

EC2

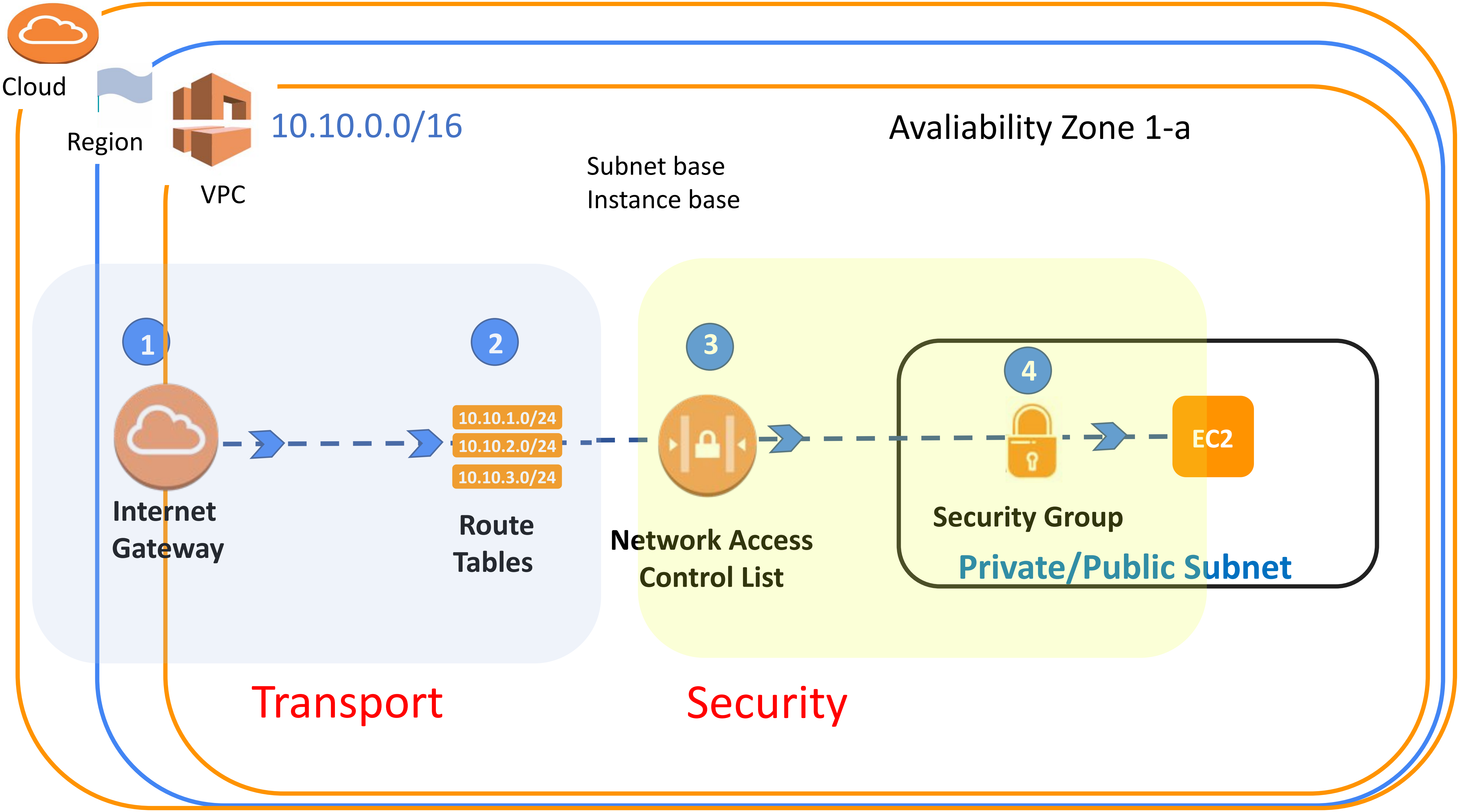
Security Group

Amazon RDS

Transport

Security

Private/Public Subnet



Cloud

Region

VPC

10.10.0.0/16

Avaliability Zone 1-a

Subnet base
Instance base

1 Internet Gateway

2 Route Tables

10.10.1.0/24
10.10.2.0/24
10.10.3.0/24

3 Network Access Control List

4 Security Group

EC2

Private/Public Subnet

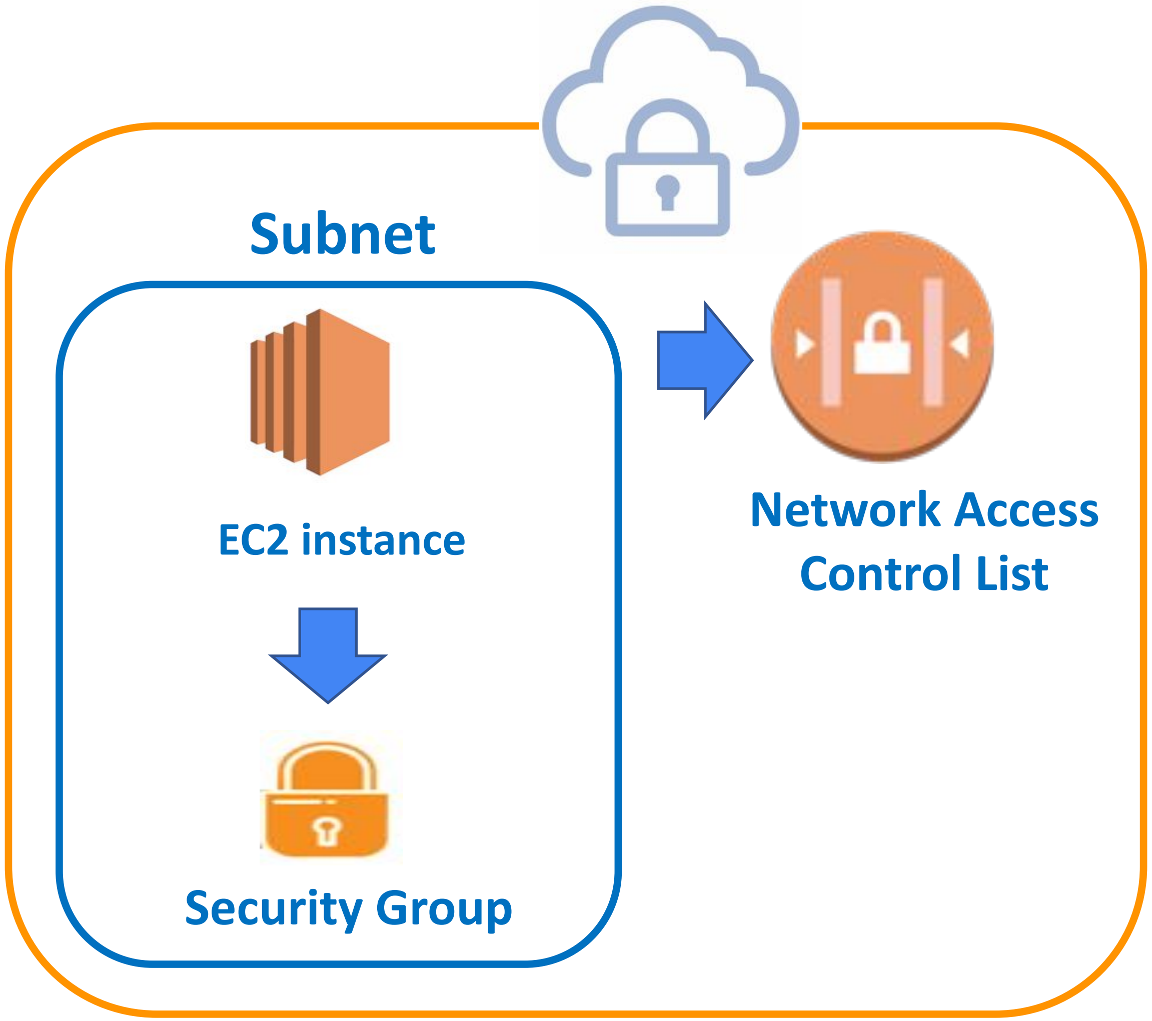
Transport

Security

NACL (NETWORK ACCESS LISTS)

Subnet obeys the NACL rules

Resources obeys NACL and Sec. Group



(Statefull) Security Group inbound

Type	Protocol	Port Range	Source
HTTP	TCP(6)	80	1.2.3.4/32
SSH-22	TCP(6)	22	0.0.0.0/0
All ICMP-IPv4	ICMP(1)	ALL	0.0.0.0/0
HTTPS	TCP(6)	443	7.8.9.10/32

ALLOW Only

Network ACL inbound (Stateless)

Rule	Type	Protocol	Port Range	Source	Allow/ Deny
100	HTTP	TCP(6)	80	7.8.9.10/32	ALLOW
200	SSH-22	TCP(6)	22	0.0.0.0/0	ALLOW
300	All ICMP-IPv4	ICMP(1)	ALL	0.0.0.0/0	ALLOW
400	HTTPS	TCP(6)	443	7.8.9.10/32	DENY
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

(Stateless) Network ACL outbound

Rule	Type	Protocol	Port Range	Destination	Allow/ Deny
100	HTTP	TCP(6)	80	7.8.9.10/32	ALLOW
200	Custom TCP	TCP(6)	32768 -65535	0.0.0.0/0	ALLOW
300	All ICMP-IPv4	ICMP(1)	ALL	0.0.0.0/0	ALLOW
400	HTTPS	TCP(6)	443	7.8.9.10/32	DENY
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

User

PC IP: 7.8.9.10/32

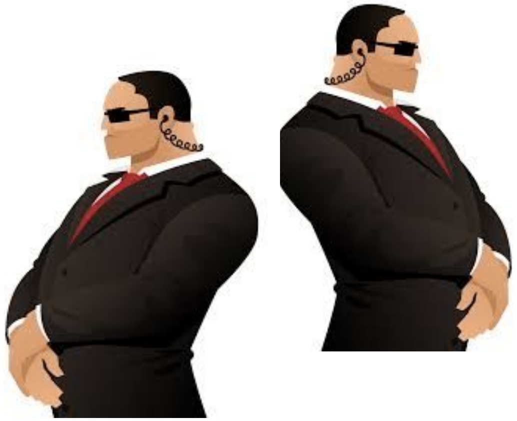
Connection Request

No	Type-Port
1	SSH-22
2	HTTP-80
3	All ICMP-IPv4 -All
4	HTTPS-443
5	Msql/Auro. 3306

EC2

Security Group inbound

Type	Protocol	Port Range	Source
HTTP	TCP(6)	80	1.2.3.4/32
SSH-22	TCP(6)	22	0.0.0.0/0
All ICMP-IPv4	ICMP(1)	ALL	0.0.0.0/0
HTTPS	TCP(6)	443	7.8.9.10/32



Subnet

Network ACL in/outbound

Rule	Type	Protocol	Port Range	Source/ Destination	Allow/ Deny
100	HTTP	TCP(6)	80	7.8.9.10/32	ALLOW
200	SSH-22	TCP(6)	22	0.0.0.0/0	ALLOW
300	All ICMP-IPv4	ICMP(1)	ALL	0.0.0.0/0	ALLOW
400	HTTPS	TCP(6)	443	7.8.9.10/32	DENY
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

User

User IP: 7.8.9.10/32

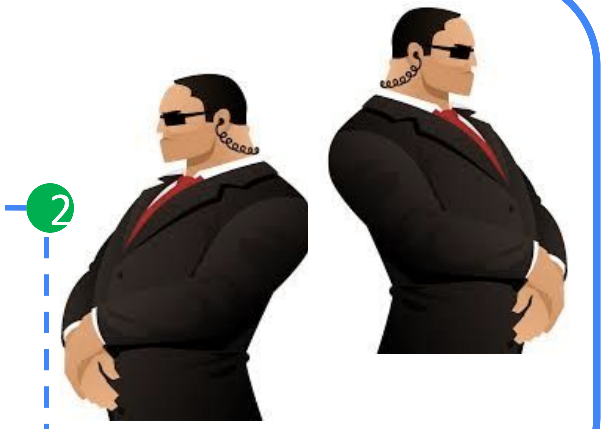
Connection Request

No	Type-Port
1	SSH-22
2	HTTP-80
3	All ICMP-IPv4 -All
4	HTTPS-443
5	Msql/Auro. 3306

EC2

Security Group inbound

Type	Protocol	Port Range	Source
HTTP	TCP(6)	80	1.2.3.4/32
SSH-22	TCP(6)	22	0.0.0.0/0
All ICMP-IPv4	ICMP(1)	ALL	0.0.0.0/0
HTTPS	TCP(6)	443	7.8.9.10/32



Network ACL in/outbound

Rule	Type	Protocol	Port Range	Source/ Destination	Allow/ Deny
100	HTTP	TCP(6)	80	7.8.9.10/32	ALLOW
200	SSH-22	TCP(6)	22	0.0.0.0/0	ALLOW
300	All ICMP-IPv4	ICMP(1)	ALL	0.0.0.0/0	ALLOW
400	HTTPS	TCP(6)	443	7.8.9.10/32	DENY
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

User

User IP: 7.8.9.10/32

Connection Request

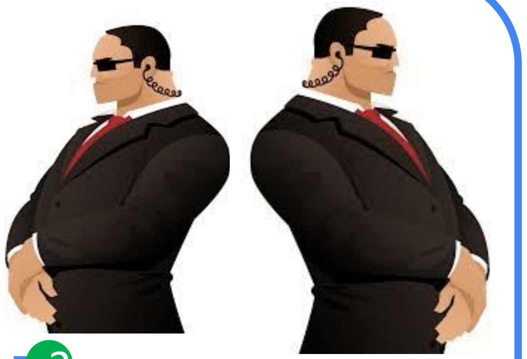
No	Type-Port
1	SSH-22
2	HTTP-80
3	All ICMP-IPv4 -All
4	HTTPS-443
5	Msql/Auro. 3306

Security Group inbound

EC2

✓ 3

Type	Protocol	Port Range	Source
HTTP	TCP(6)	80	1.2.3.4/32
SSH-22	TCP(6)	22	0.0.0.0/0
All ICMP-IPv4	ICMP(1)	ALL	0.0.0.0/0
HTTPS	TCP(6)	443	7.8.9.10/32



3

Network ACL in/outbound

3 3 3

Rule	Type	Protocol	Port Range	Source/ Destination	Allow/ Deny
100	HTTP	TCP(6)	80	7.8.9.10/32	ALLOW
200	SSH-22	TCP(6)	22	0.0.0.0/0	ALLOW
300	All ICMP-IPv4	ICMP(1)	ALL	0.0.0.0/0	ALLOW
400	HTTPS	TCP(6)	443	7.8.9.10/32	DENY
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

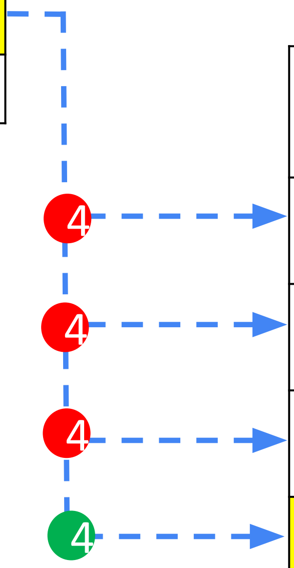
3

User

User IP: 7.8.9.10/32

Connection Request

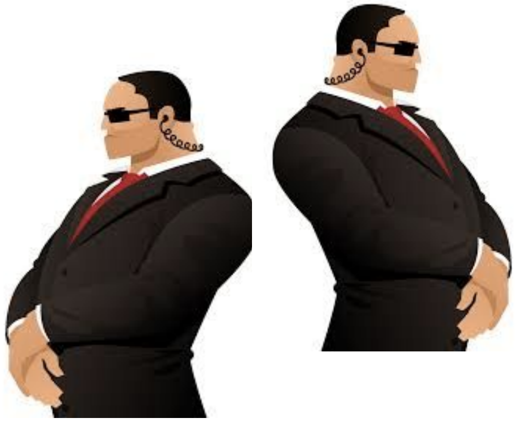
No	Type-Port
1	SSH-22
2	HTTP-80
3	All ICMP-IPv4 -All
4	HTTPS-443
5	Msql/Auro. 3306



EC2

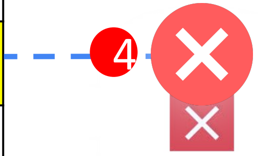
Security Group inbound

Type	Protocol	Port Range	Source
HTTP	TCP(6)	80	1.2.3.4/32
SSH-22	TCP(6)	22	0.0.0.0/0
All ICMP-IPv4	ICMP(1)	ALL	0.0.0.0/0
HTTPS	TCP(6)	443	7.8.9.10/32



Network ACL in/outbound

Rule	Type	Protocol	Port Range	Source/ Destination	Allow/ Deny
100	HTTP	TCP(6)	80	7.8.9.10/32	ALLOW
200	SSH-22	TCP(6)	22	0.0.0.0/0	ALLOW
300	All ICMP-IPv4	ICMP(1)	ALL	0.0.0.0/0	ALLOW
400	HTTPS	TCP(6)	443	7.8.9.10/32	DENY
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY



User

User IP: 7.8.9.10/32

Connection Request

No	Type-Port
1	SSH-22
2	HTTP-80
3	All ICMP-IPv4 -All
4	HTTPS-443
5	Msql/Auro. 3306

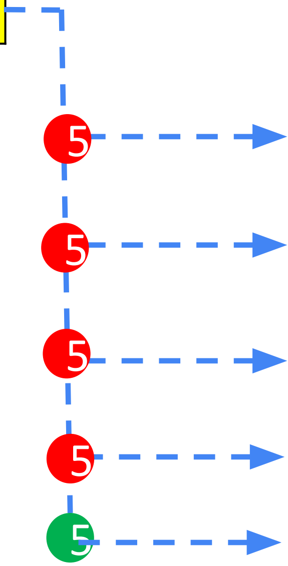
EC2

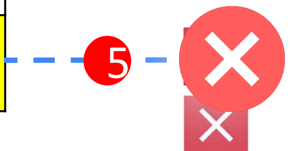
Security Group inbound

Type	Protocol	Port Range	Source
HTTP	TCP(6)	80	1.2.3.4/32
SSH-22	TCP(6)	22	0.0.0.0/0
All ICMP-IPv4	ICMP(1)	ALL	0.0.0.0/0
HTTPS	TCP(6)	443	7.8.9.10/32

Network ACL in/outbound

Rule	Type	Protocol	Port Range	Source/ Destination	Allow/ Deny
100	HTTP	TCP(6)	80	7.8.9.10/32	ALLOW
200	SSH-22	TCP(6)	22	0.0.0.0/0	ALLOW
300	All ICMP-IPv4	ICMP(1)	ALL	0.0.0.0/0	ALLOW
400	HTTPS	TCP(6)	443	7.8.9.10/32	DENY
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY





EPHEMERAL PORT

NACLs are stateless. This means that you are required to have a rule for inbound AND outbound traffic. So, if you want to allow your EC2 instance to serve HTTP traffic, you will need to allow port 80 inbound and ports 1024 – 65535 outbound. But where 1024 – 65535 came from.

The ports 1024 – 65535 are called the “ephemeral ports”.

These ports are randomly selected to allow return traffic for a request. So, if a request comes to the server on port 80, the request also specifies a random port between 1024 – 65535 for the return traffic.

NACL TABLES

Let's get our hands dirty!

- NACL Tables

THANKS!

Any questions?