Amazon VPC-4

CLARUSWAY
WAY TO REINVENT YOURSELF

Table of Content

WORDPRESS WITH LAMP STACK ON VPC

Dynamic Website

Dynamic Website

Operating System
eg: linux or windows

Web Server
eg: apache, nginx

Database
eg: mysql, aurora

Progr. Language
eg: PHP, NodeJS

What is WordPress?

At its core, WordPress is the simplest, most popular way to create your own website or blog. In fact, WordPress powers over 43.3% of all the websites on the Internet. Yes – more than one in four websites that you visit are likely powered by WordPress.

Setup Wordpress with Database

Operating System

Web Server

Database

Progr. language

User Data

LAMP:

Installed-ready

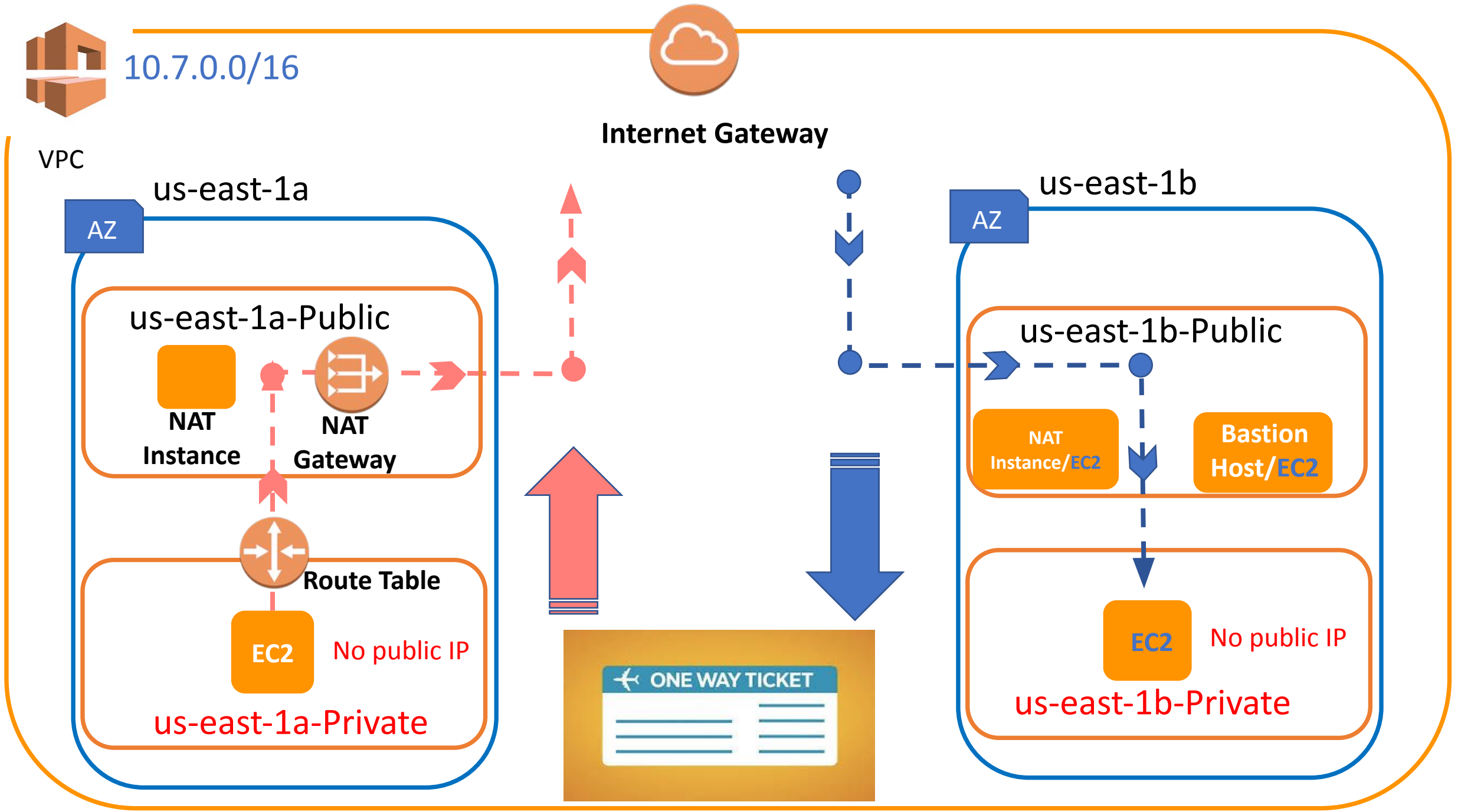
EC2 Amazon Linux 2

User Data

User Data

User Data

User Data


10.7.0.0/16
Internet Gateway
VPC
us-east-1a
AZ
us-east-1a-Public
NAT Instance
NAT Gateway
Route Table
EC2
No public IP
us-east-1a-Private
ONE WAY TICKET
us-east-1b
AZ
us-east-1b-Public
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

EC2 Amazon Linux 2

User Data

User Data

User Data

?

v

v

It is in another instance in the Private Subnet

1- Desired Scenario

Cloud

Region

Clarus-VPC-a

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

1- Desired Scenario

Cloud

Region

Clarus-VPC-a

Internet Gateway

Avaliability Zone 1-a

Public Subnet 1a

NAT GATEWAY

Private Subnet 1a

Avaliability Zone 1-b

Public Subnet 1b

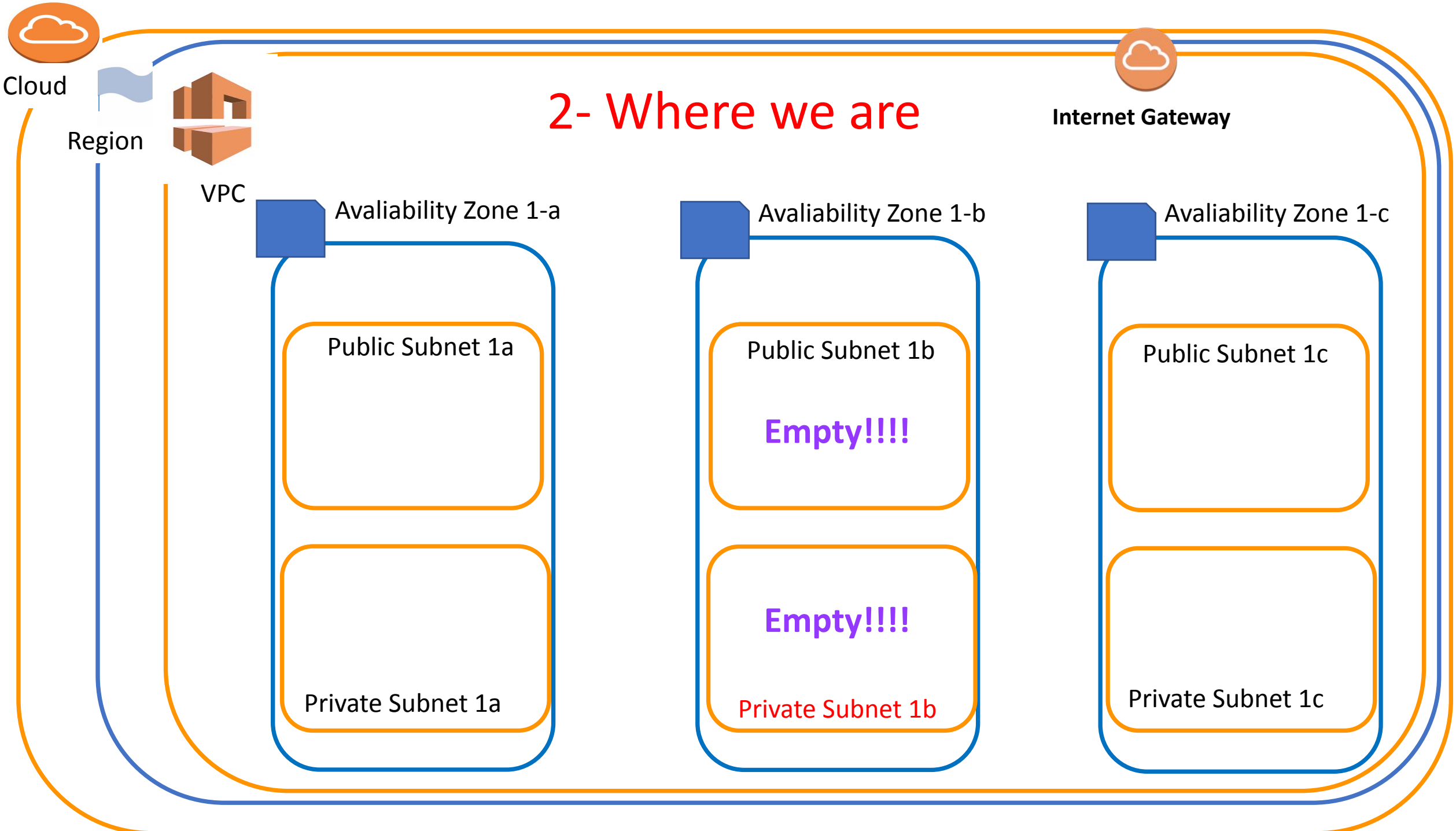
Private Subnet 1b

Avaliability Zone 1-c

Public Subnet 1c

BASTION HOST

Private Subnet 1c


Cloud
Region
VPC
2- Where we are
Internet Gateway
Avaliability Zone 1-a
Avaliability Zone 1-b
Avaliability Zone 1-c
Public Subnet 1a
Public Subnet 1b
Empty!!!!
Public Subnet 1c
Empty!!!!
Private Subnet 1a
Private Subnet 1b
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

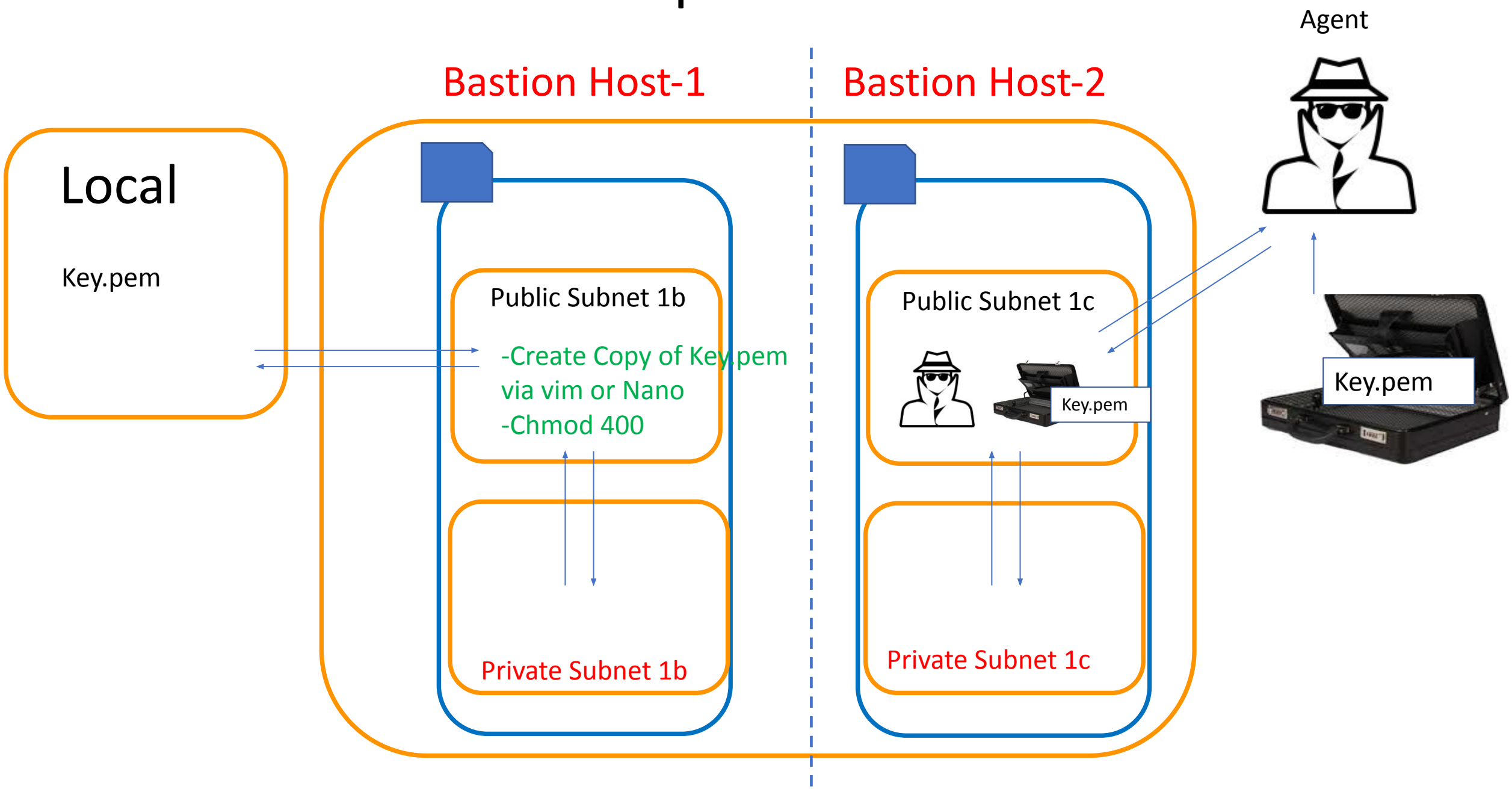
Private Subnet 1b

Availability Zone 1-c

Public Subnet 1c

Private Subnet 1c

.pem Issue


Agent
Bastion Host-1
Bastion Host-2
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

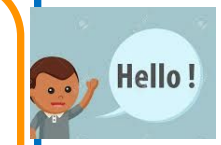
Avaliability Zone 1-a

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

Cloud

Region

VPC

Internet Gateway

3- Try to install mariaDB

Public Subnet 1a

Private Subnet 1a

1

Bastion Host

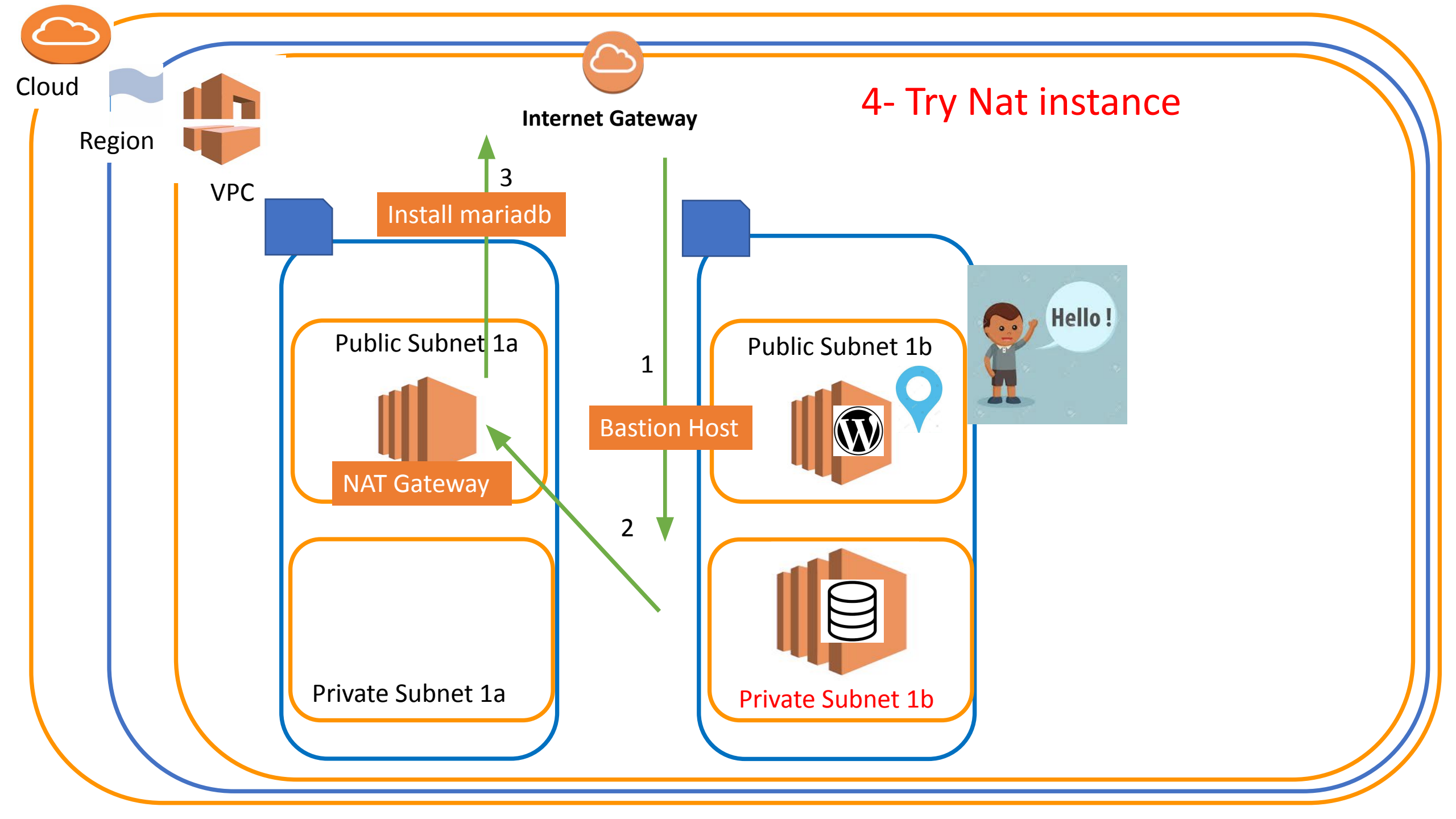
2

Install mariadb

Public Subnet 1b

Private Subnet 1b

4- Try Nat instance



5- Associate DATABASE

Cloud

Region

VPC

Internet Gateway

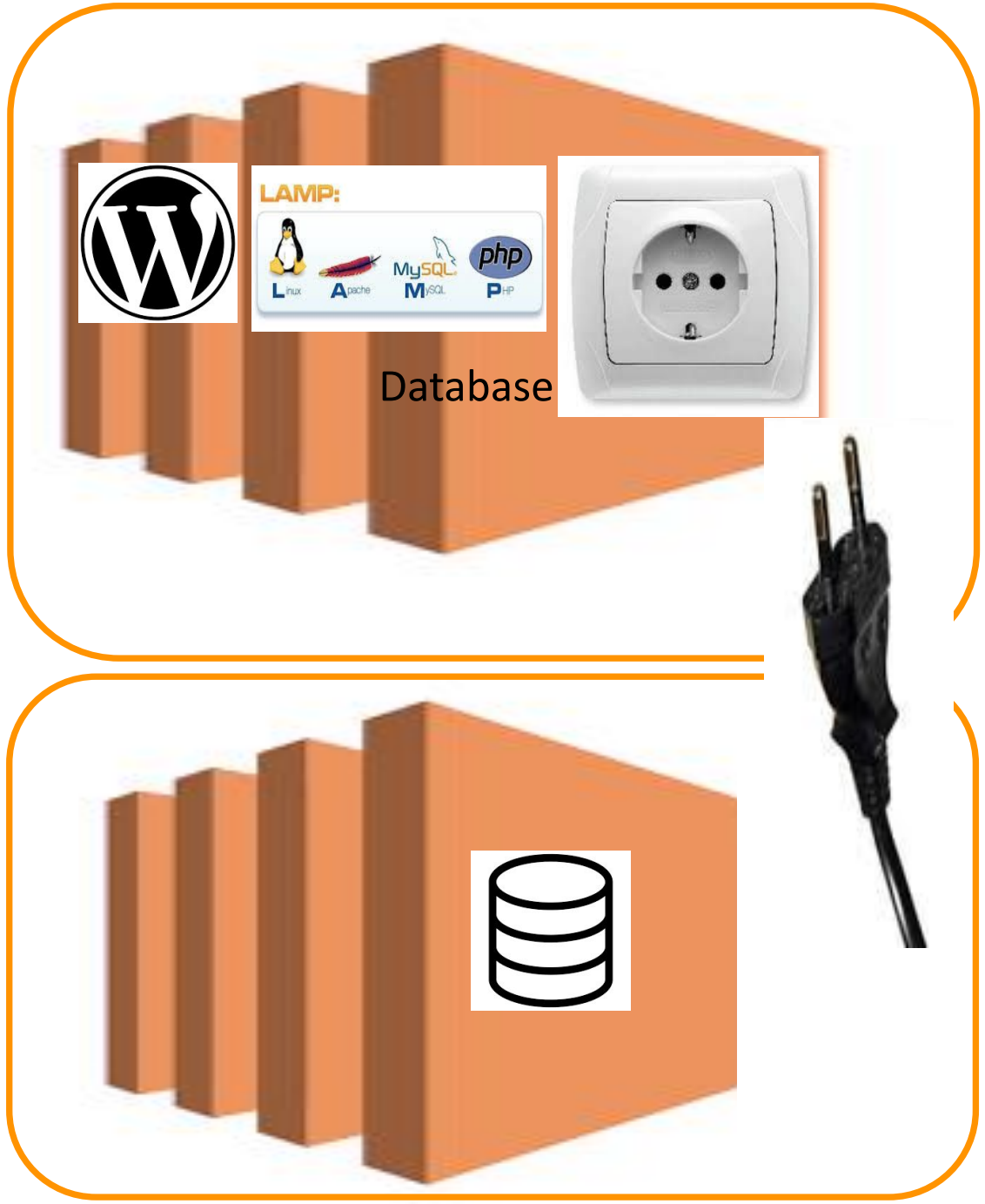
Public Subnet 1a

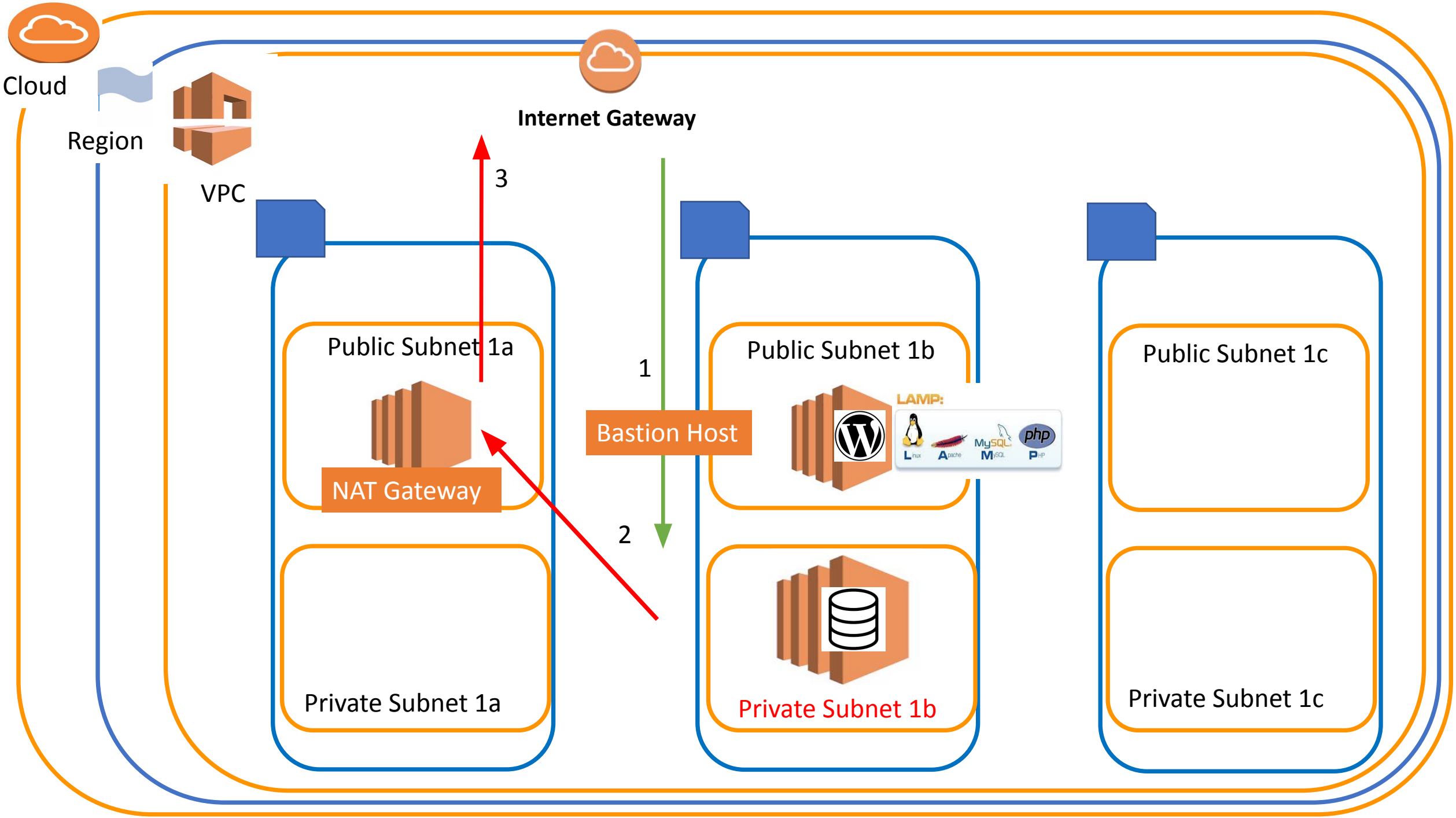
Private Subnet 1a

Public Subnet 1b

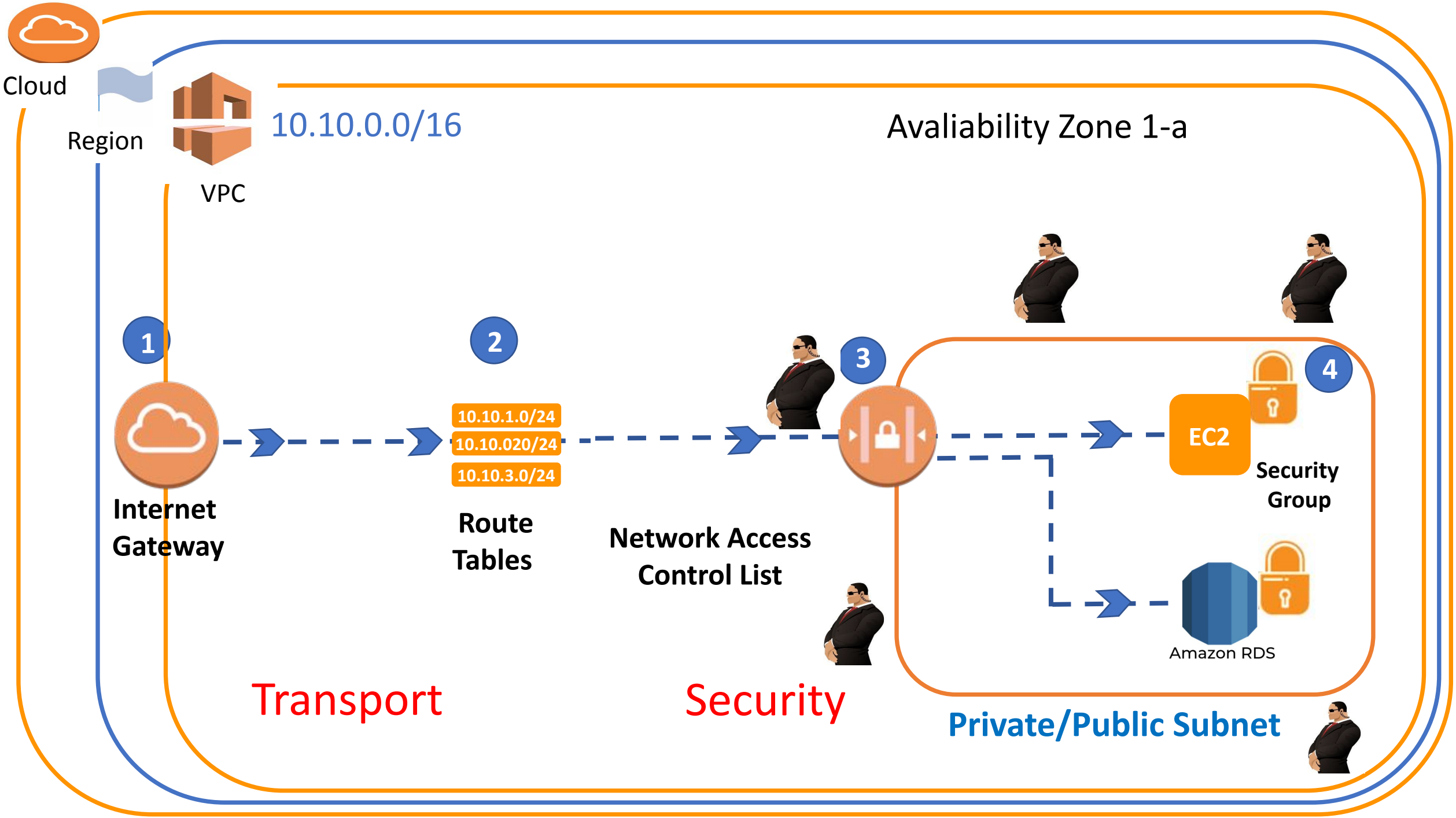
Private Subnet 1b

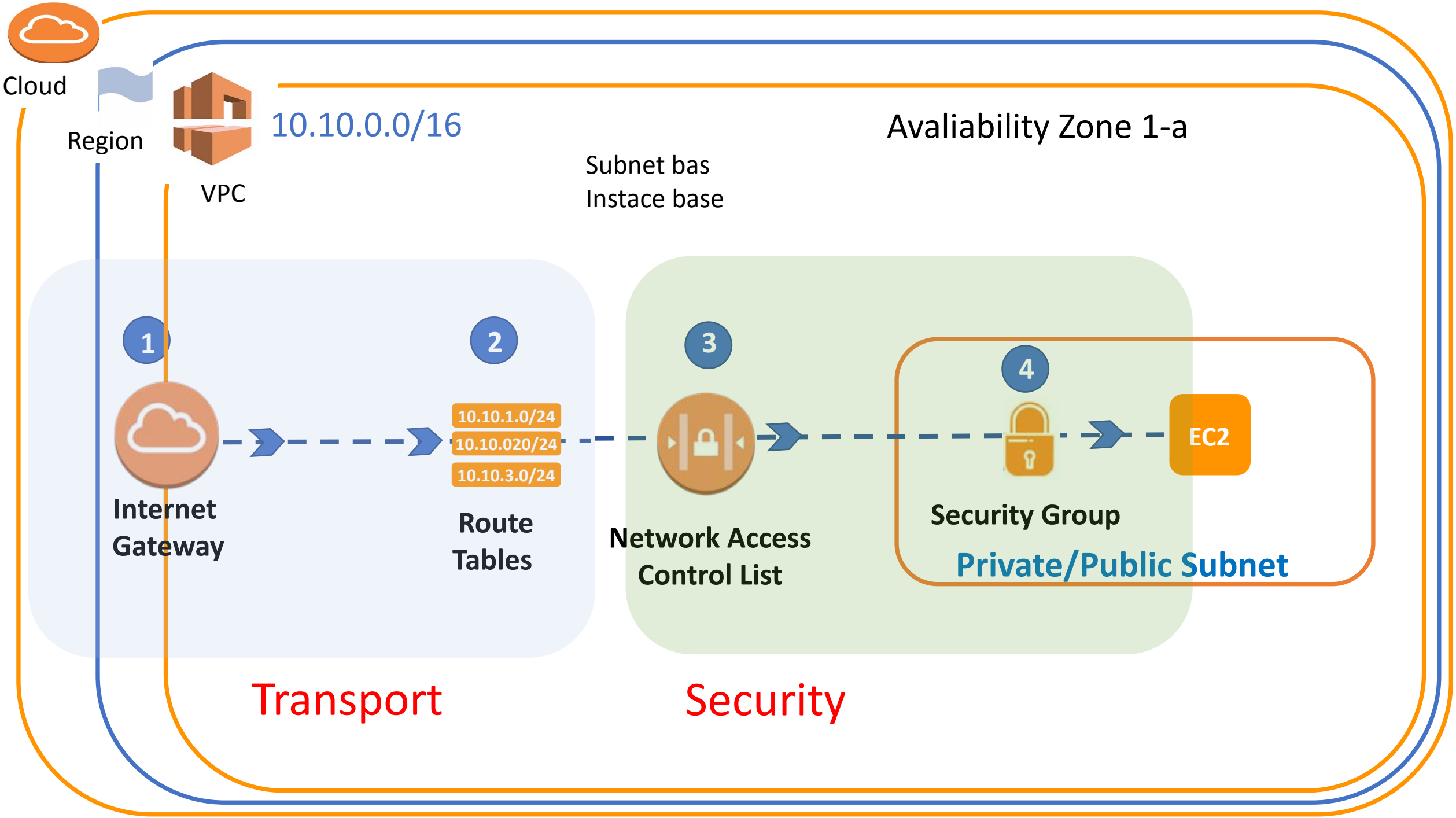
Associate DATABASE




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

NACL (NETWORK ACCESS LISTS)

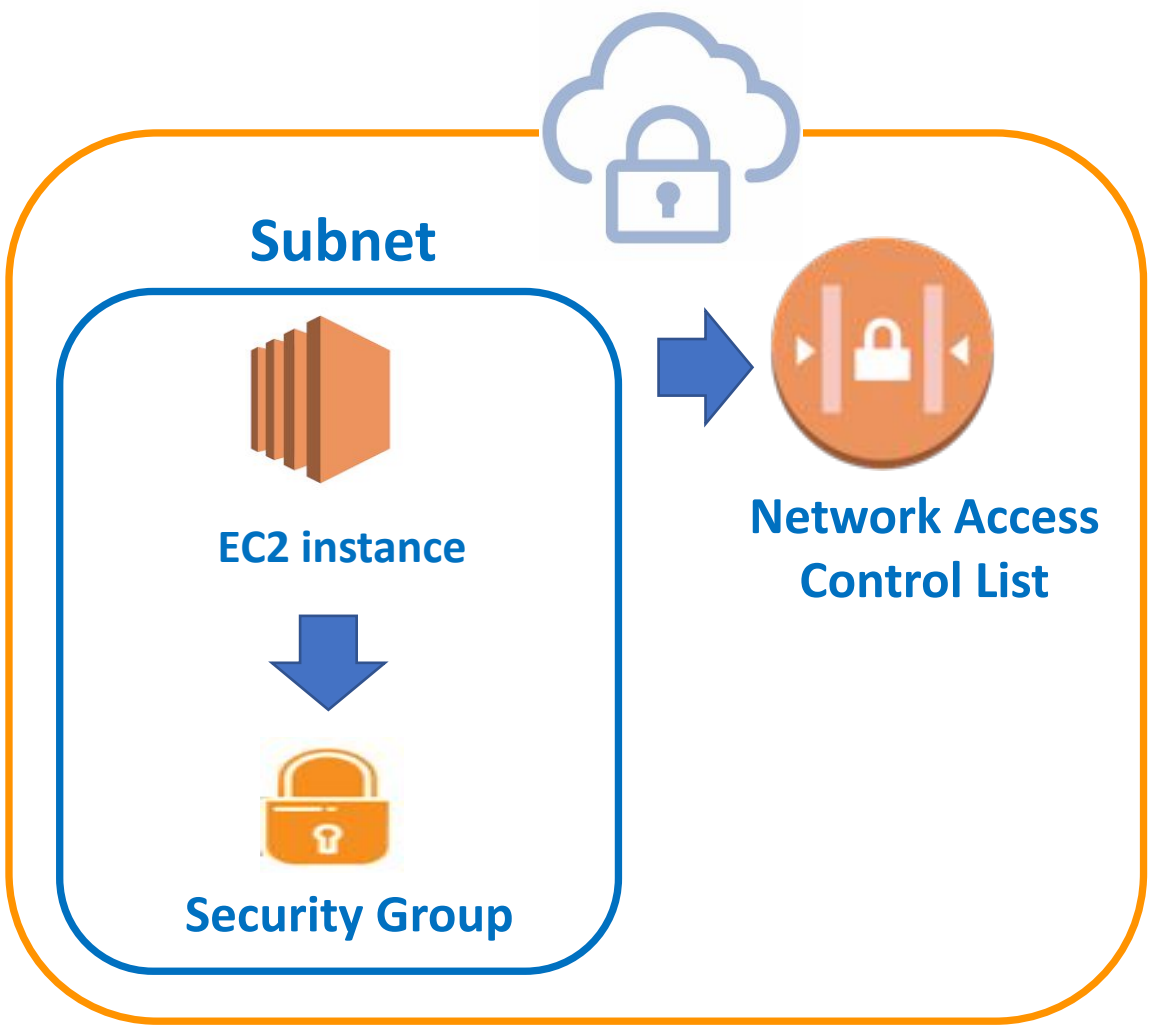

Cloud
Region
VPC
10.10.0.0/16
Avaliability Zone 1-a
1
2
3
4
10.10.1.0/24
10.10.020/24
10.10.3.0/24
Internet Gateway
Route Tables
Network Access Control List
EC2
Security Group
Amazon RDS
Transport
Security
Private/Public Subnet


Cloud
Region
VPC
10.10.0.0/16
Avaliability Zone 1-a
Subnet bas
Instace base
1
2
3
4
10.10.1.0/24
10.10.020/24
10.10.3.0/24
EC2
Internet Gateway
Route Tables
Network Access Control List
Security Group
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

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

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 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

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

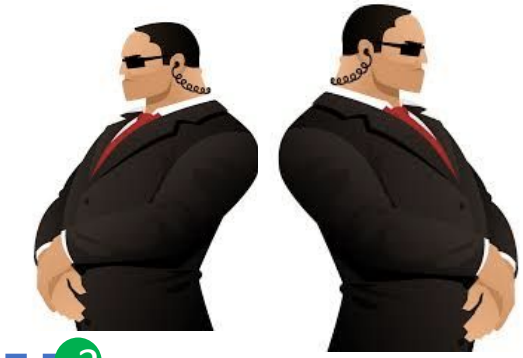
User IP: 7.8.9.10/32

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

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

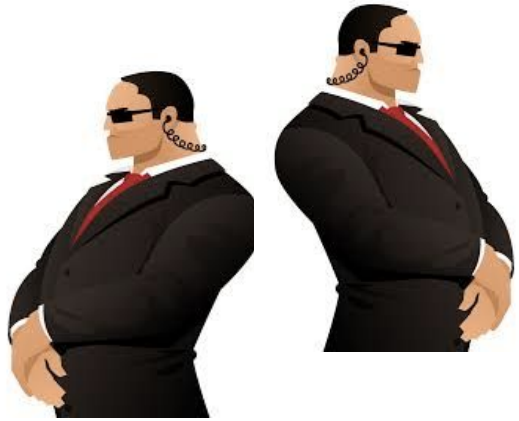
User IP: 7.8.9.10/32

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

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

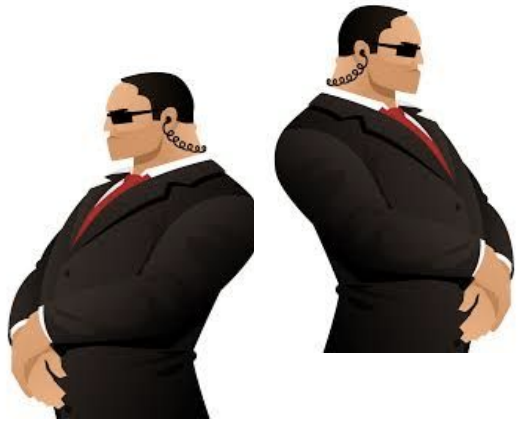
User IP: 7.8.9.10/32

Connection Request

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

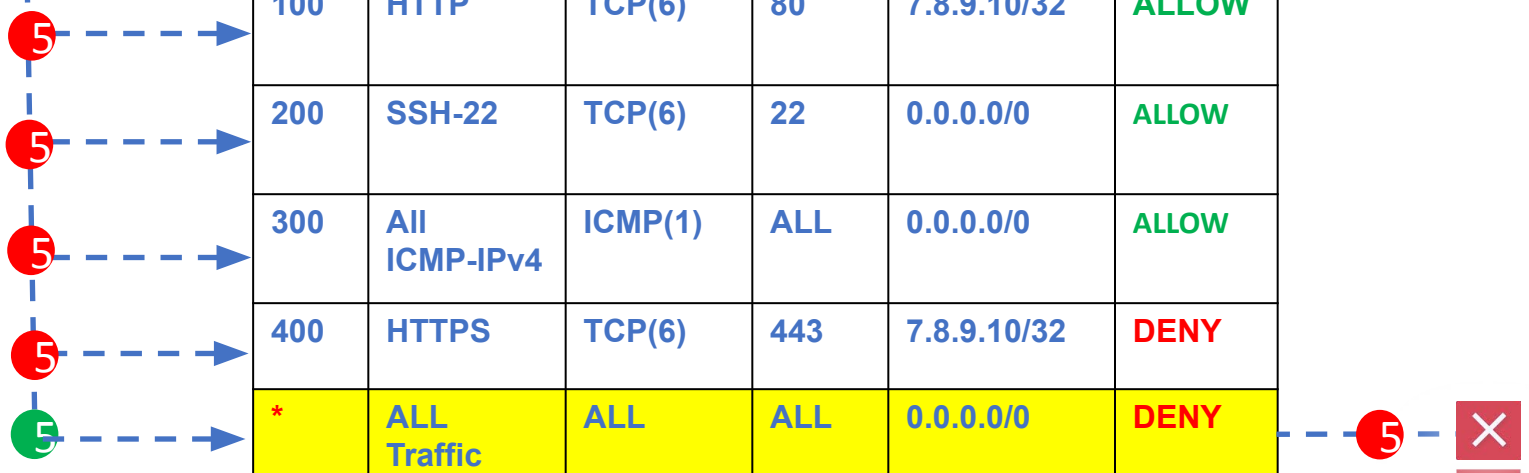
Security Group inbound

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!

- LAMP Installation
- NACL Tables

THANKS!

Any questions?

You can find me at:

- @sumod
- sumod@clarusway.com