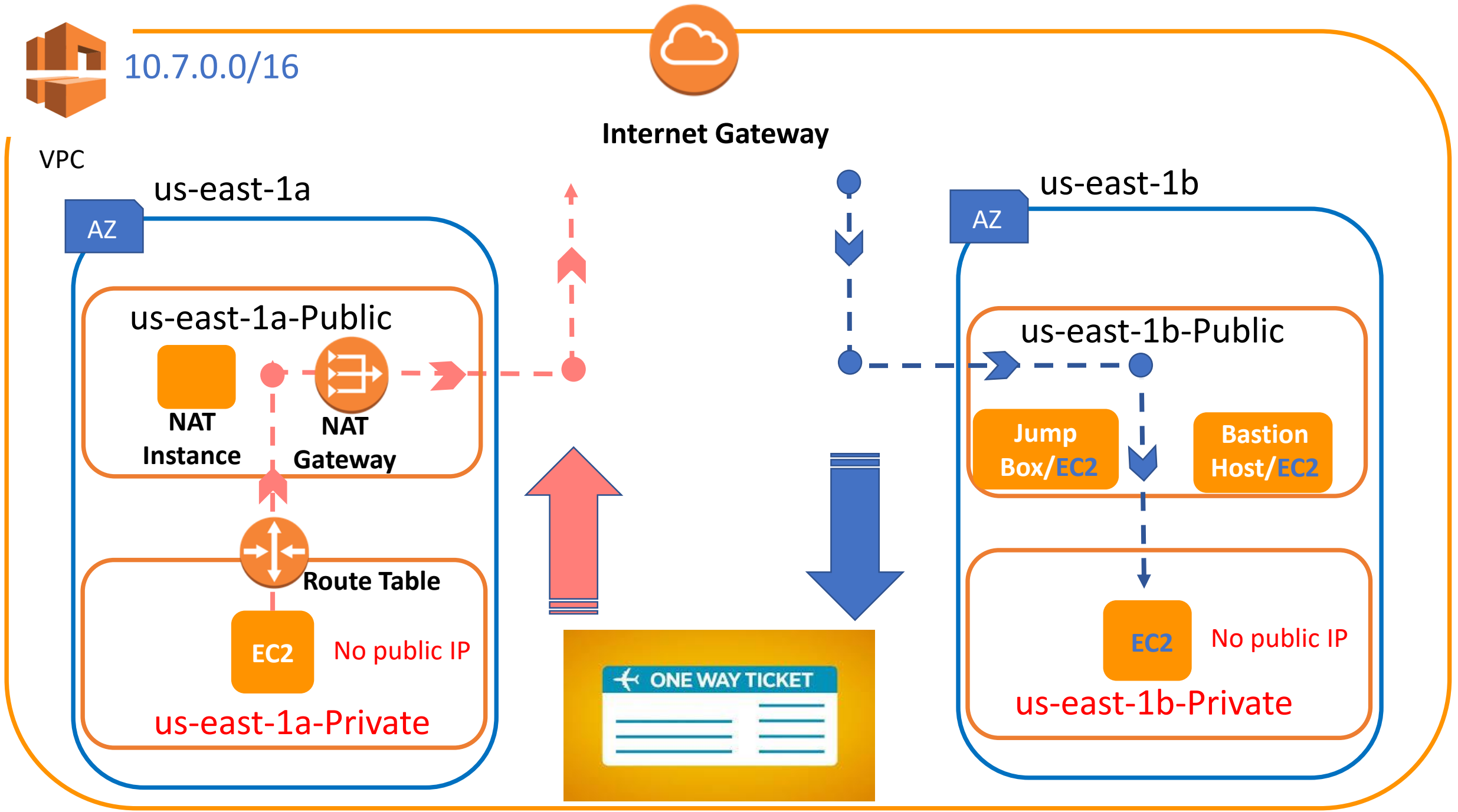

10.7.0.0/16
Internet Gateway
VPC
us-east-1a
AZ
us-east-1a-Public
NAT Instance
NAT Gateway
Route Table
EC2
No public IP
us-east-1a-Private
ONE WAY TICKET
us-east-1b
AZ
us-east-1b-Public
Jump Box/EC2
Bastion Host/EC2
EC2
No public IP
us-east-1b-Private

Dynamic Website

Operating System

Web Server

Database

Prg. Language

Setup Wordpress with Database

LAMP stands for Linux, Apache, MySQL, and PHP. LAMP is an open source Web development platform Linux is the operating system with **Apache** web server and **MySQL** Database that uses **PHP** to process dynamic website content.

Operating System | Web Server | Database | Progr. language

User Data

LAMP: ✓

Installed-ready

EC2 Amazon Linux 2 ✓

Ready

User Data ✓

Installed-ready

?

v

v

User Data ✓

Installed-ready

User Data ✓

Installed-ready

It is in another instance in the private Subnet

Cloud

Region

Clarus-VPC-a

1- Desired

Internet Gateway

Avaliability Zone 1-a

Public Subnet 1a

Private Subnet 1a

Avaliability Zone 1-b

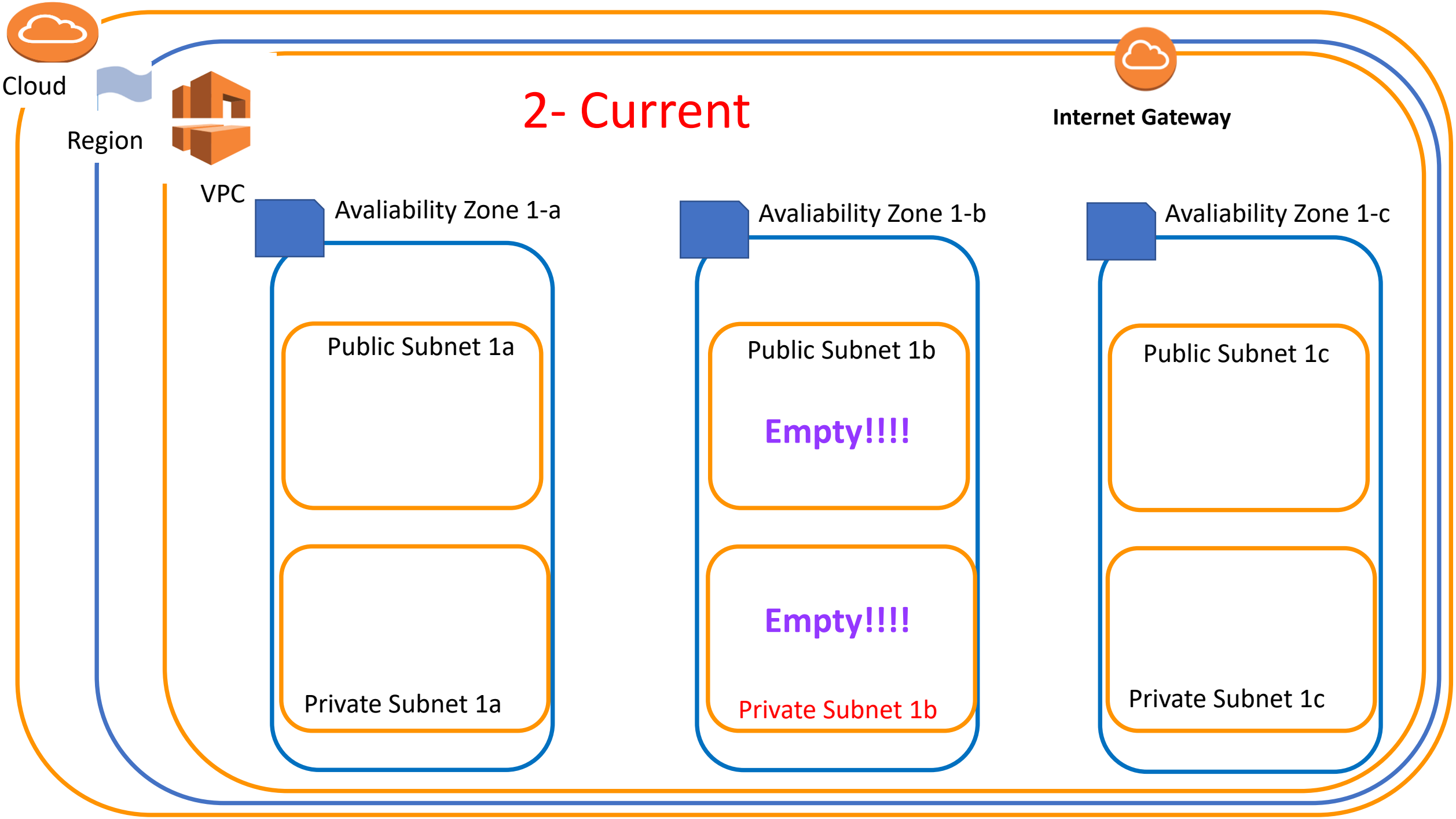
Public Subnet 1b

Private Subnet 1b

Avaliability Zone 1-c

Public Subnet 1c

Private Subnet 1c


Cloud
Region
VPC
2- Current
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

Avaliability Zone 1-a

Public Subnet 1a

Private Subnet 1a

Avaliability Zone 1-b

Public Subnet 1b

Private Subnet 1b

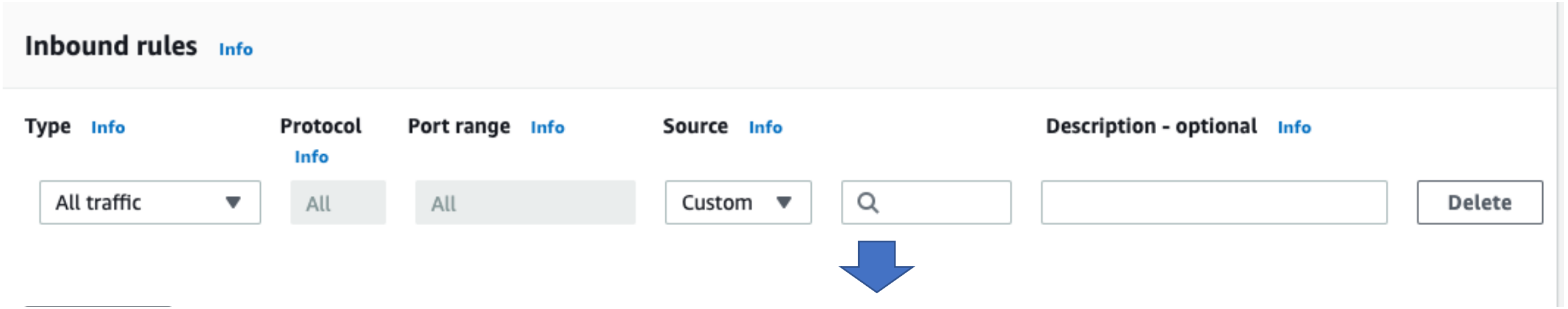
Avaliability Zone 1-c

Public Subnet 1c

Private Subnet 1c

Sec. Group Issue

Bastion Host

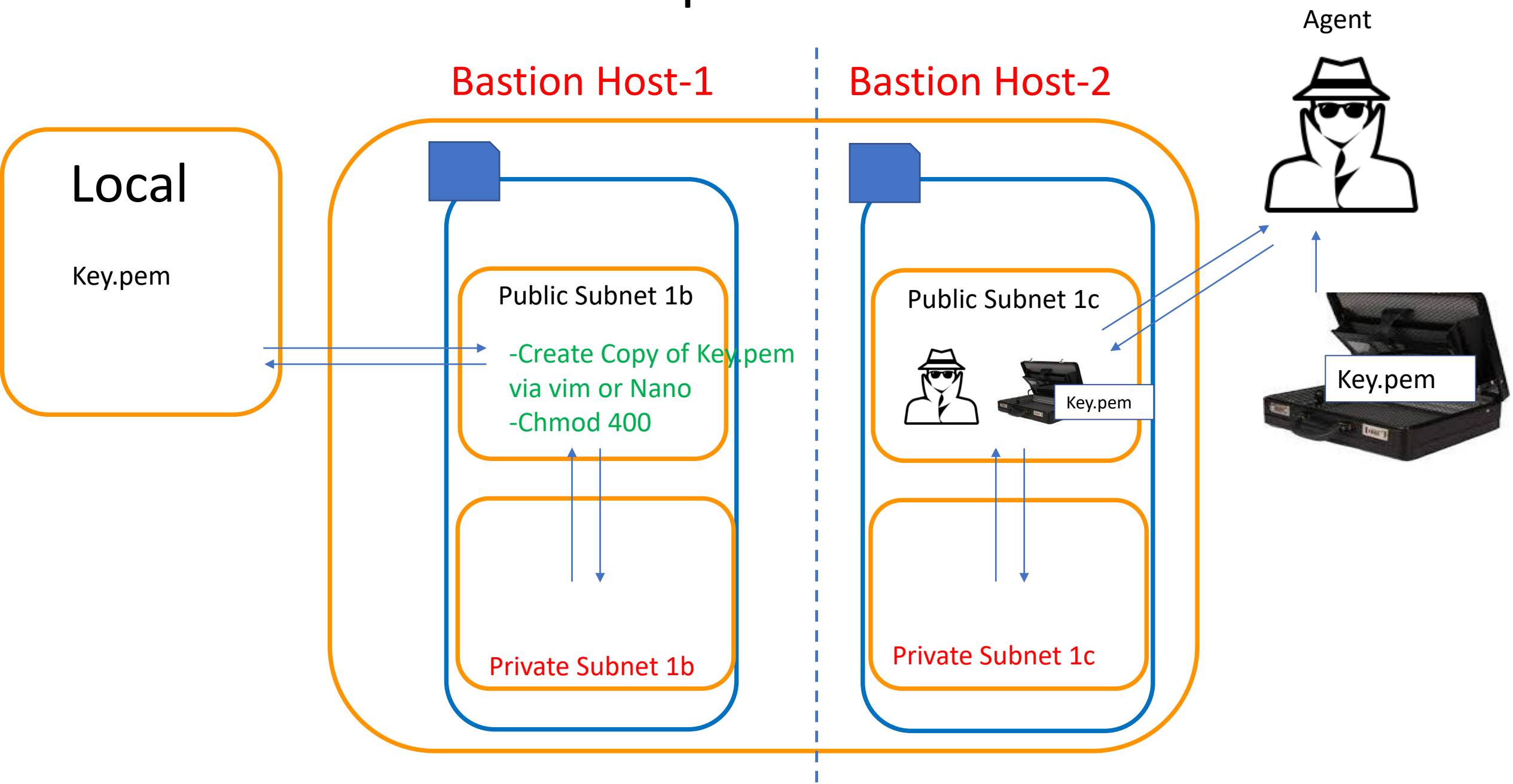


1-Sec. group of Bastion Host –Best practice

2-CIDR Block of “Public Subnet”

3-IP of Bastion Host Instance

.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

3- Try to install mariaDB

Cloud

Region

VPC

Internet Gateway

Public Subnet 1a

Private Subnet 1a

1

Bastion Host

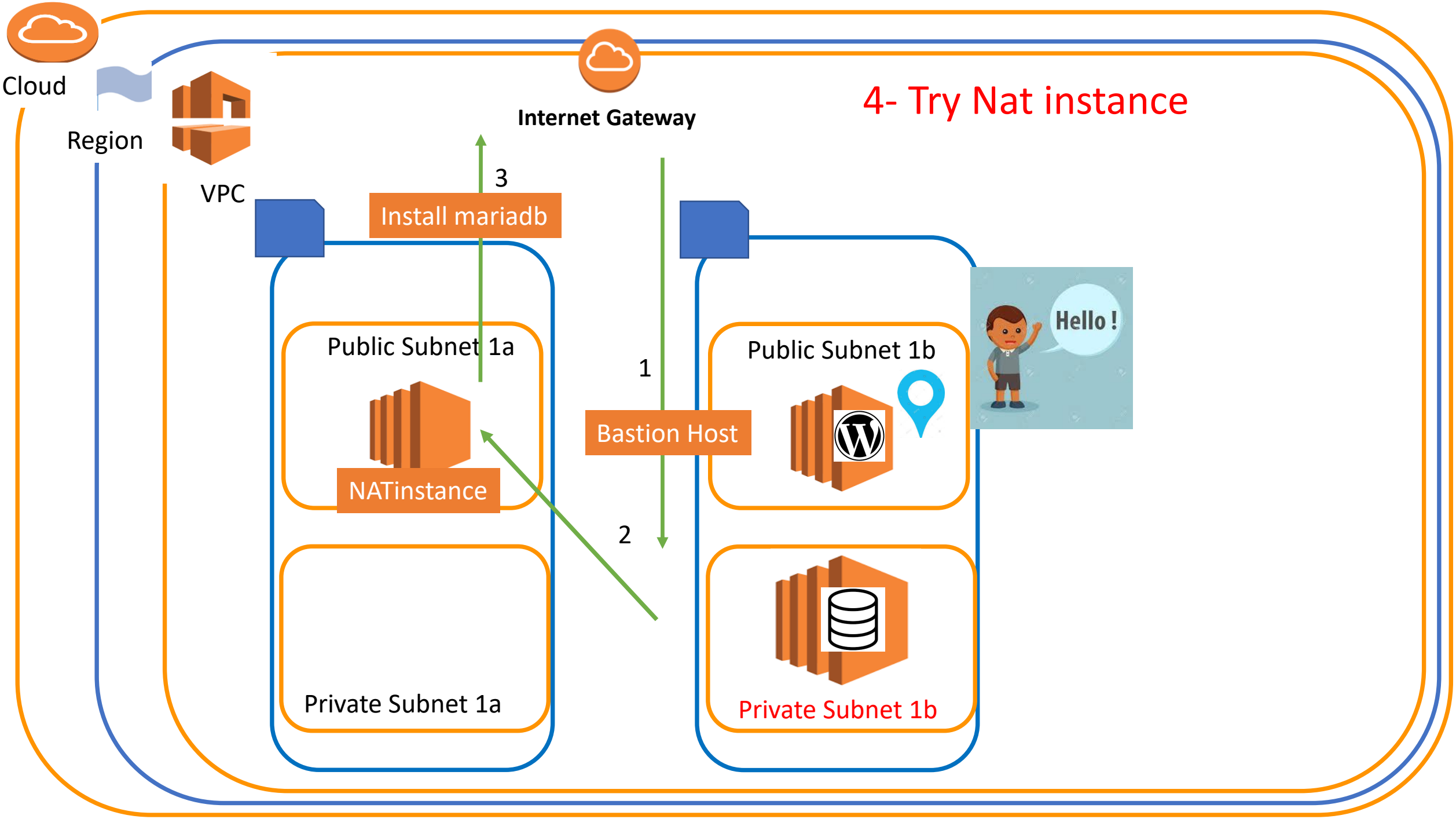
Public Subnet 1b

2

Install mariadb

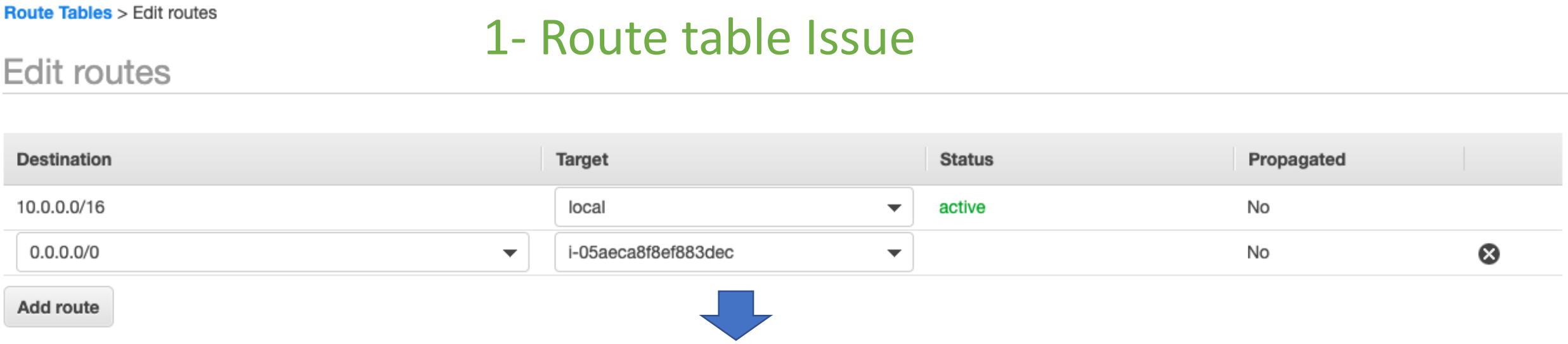
Private Subnet 1b

4- Try Nat instance



Nat instance

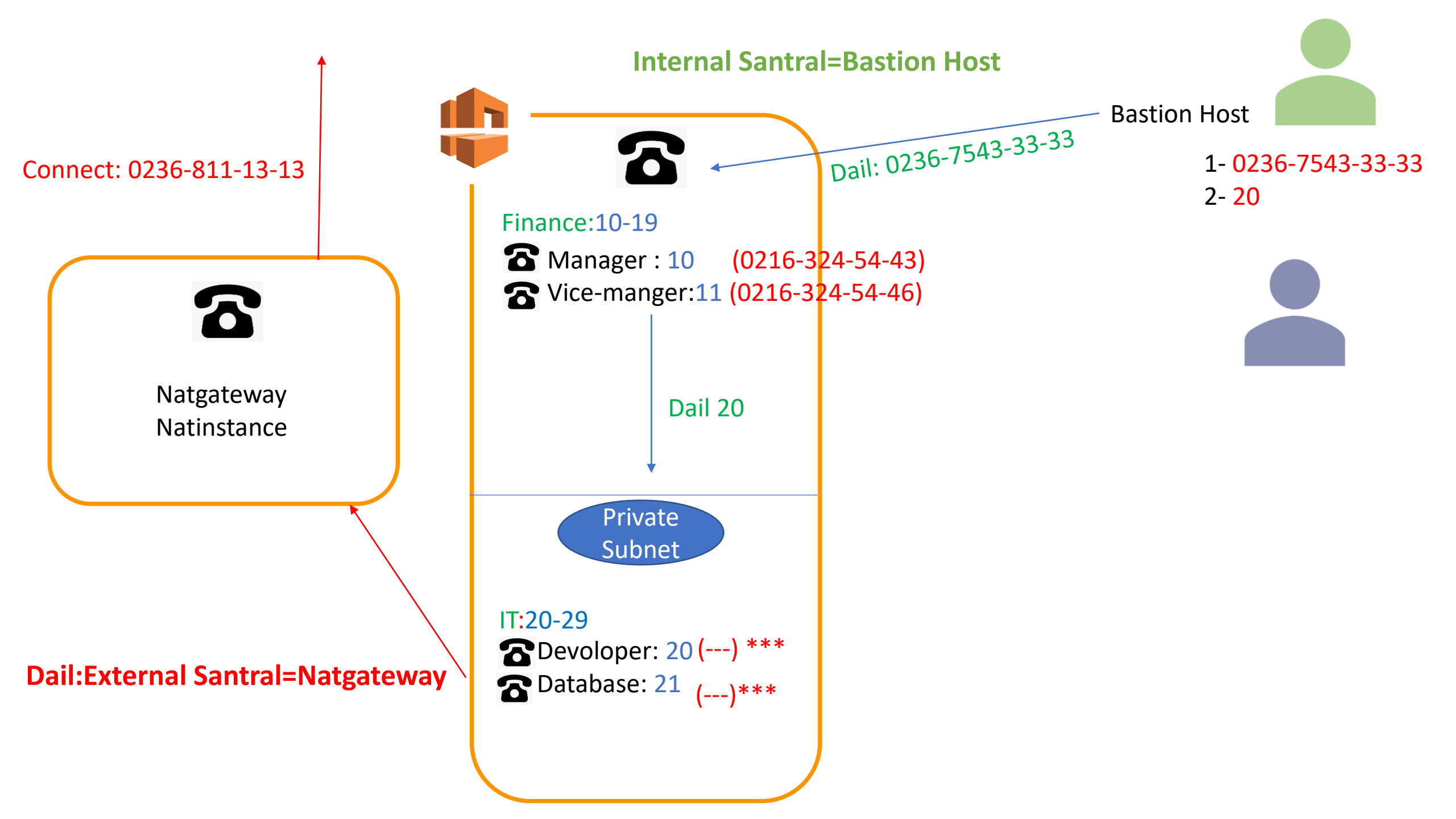
1- Route table Issue



- Nat instance

2- Change Source/ Destination Check

- Disable


Internal Santral=Bastion Host
Bastion Host
1- 0236-7543-33-33
2- 20
Dail: 0236-7543-33-33
Connect: 0236-811-13-13
Natgateway
Natinstance
Finance:10-19
Manager : 10 (0216-324-54-43)
Vice-manger:11 (0216-324-54-46)
Dail 20
Private Subnet
IT:20-29
Devoloper: 20 (---) ***
Database: 21 (---)***
Dail:External Santral=Natgateway

5- Associate DATABASE

Cloud

Region

VPC

Internet Gateway

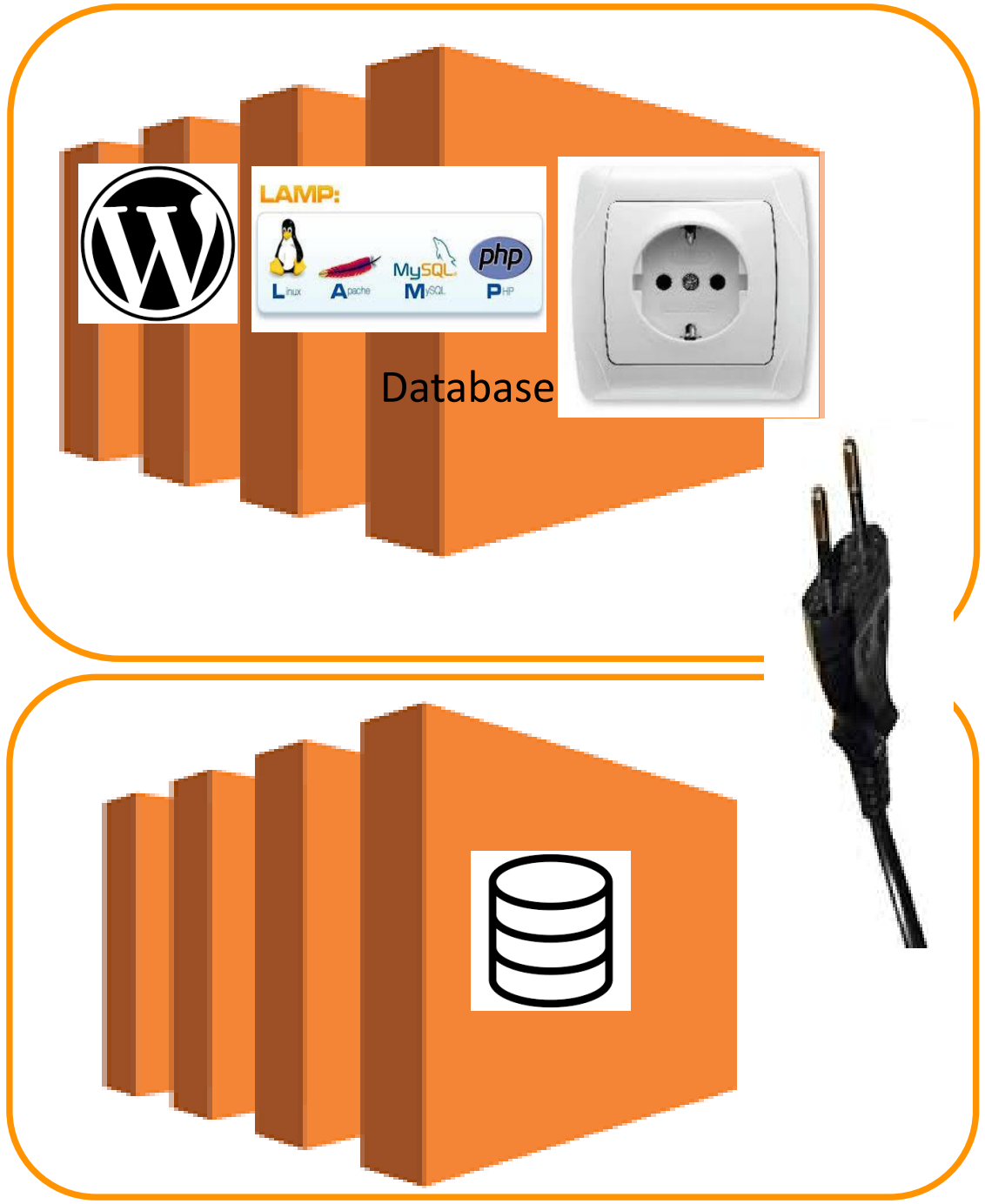
Public Subnet 1a

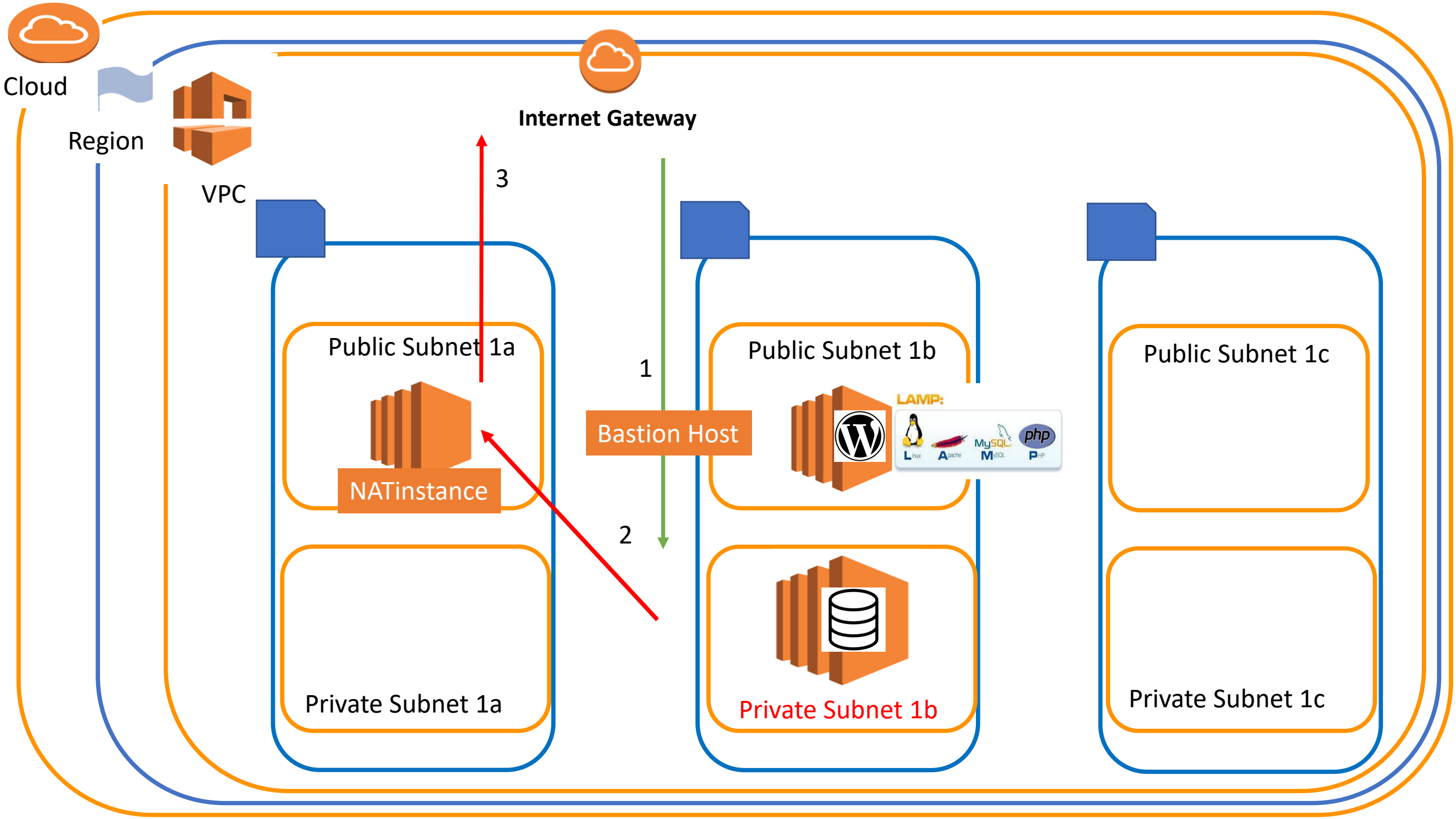
Private Subnet 1a

Public Subnet 1b

Private Subnet 1b

Associate DATABASE




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

Conclusion

Nat gateway-Nat instance

Change Route table of Private Subnet

Helps Private instance to install software package*

Nat instance/gatway = Unique instance

Bastion Host

Change Sec. Group

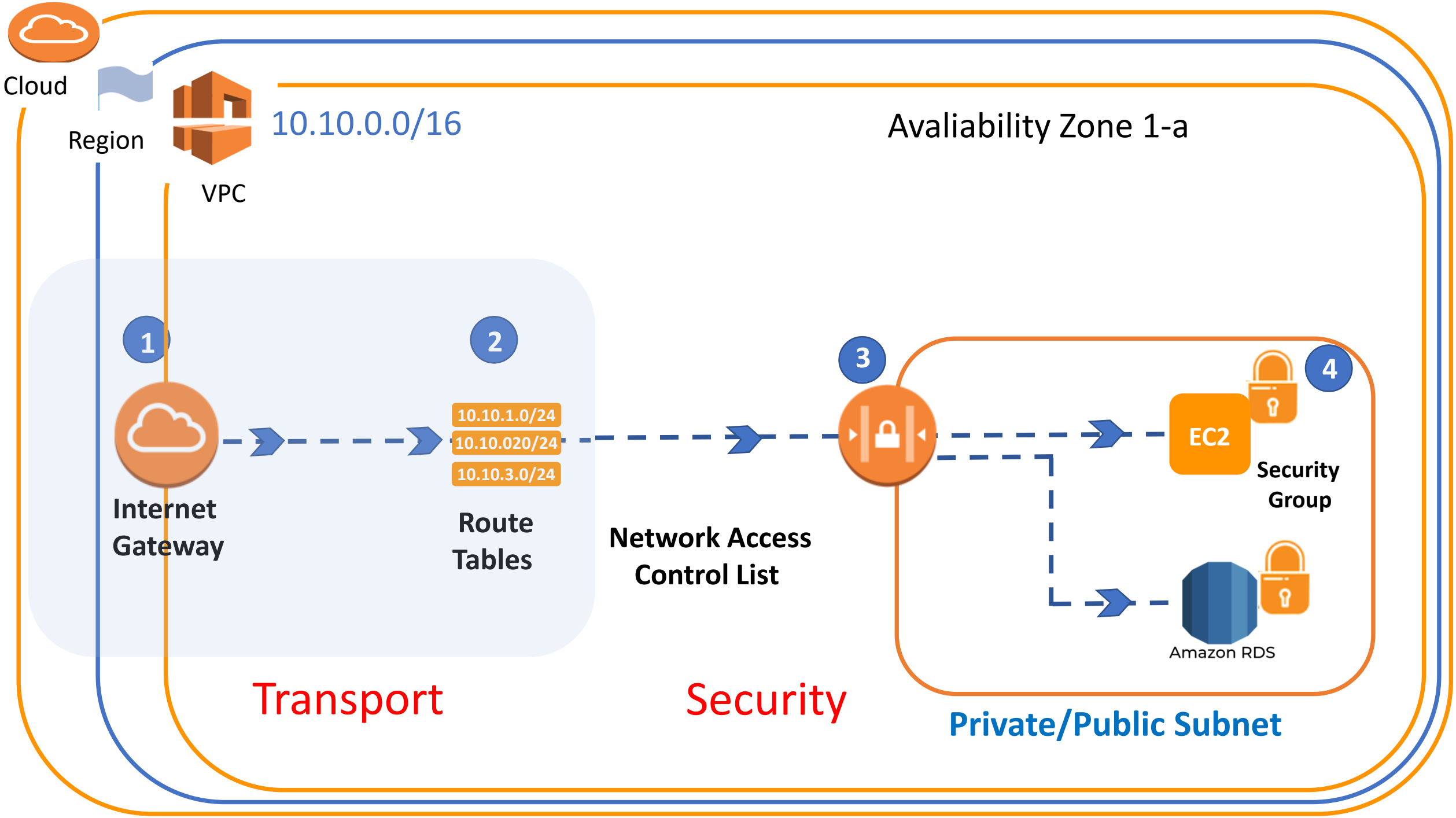
Helps Public Instance to connect Pirvate instance

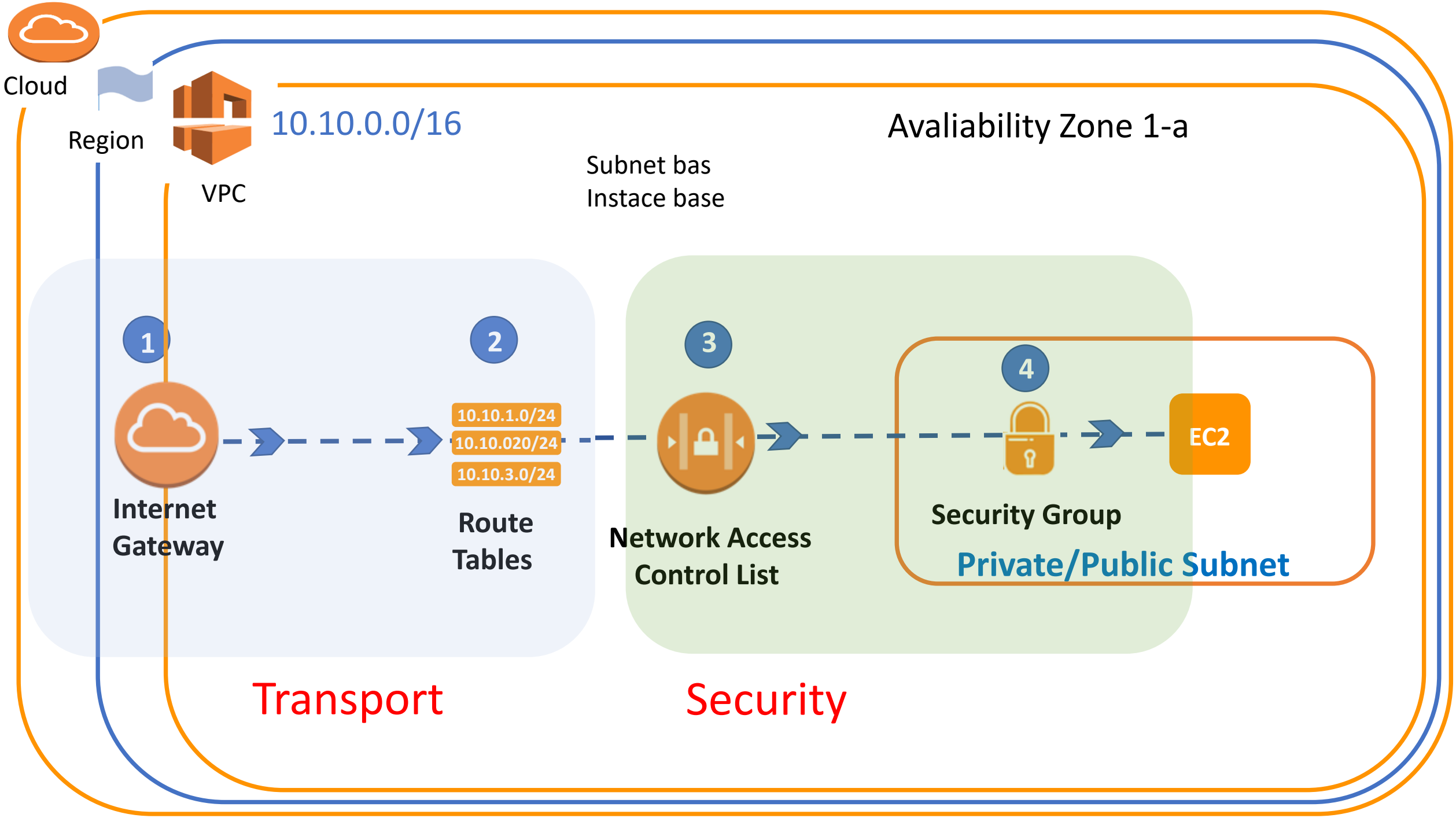
Bastion Host = Ordinary instance in public Subnet

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

NACL

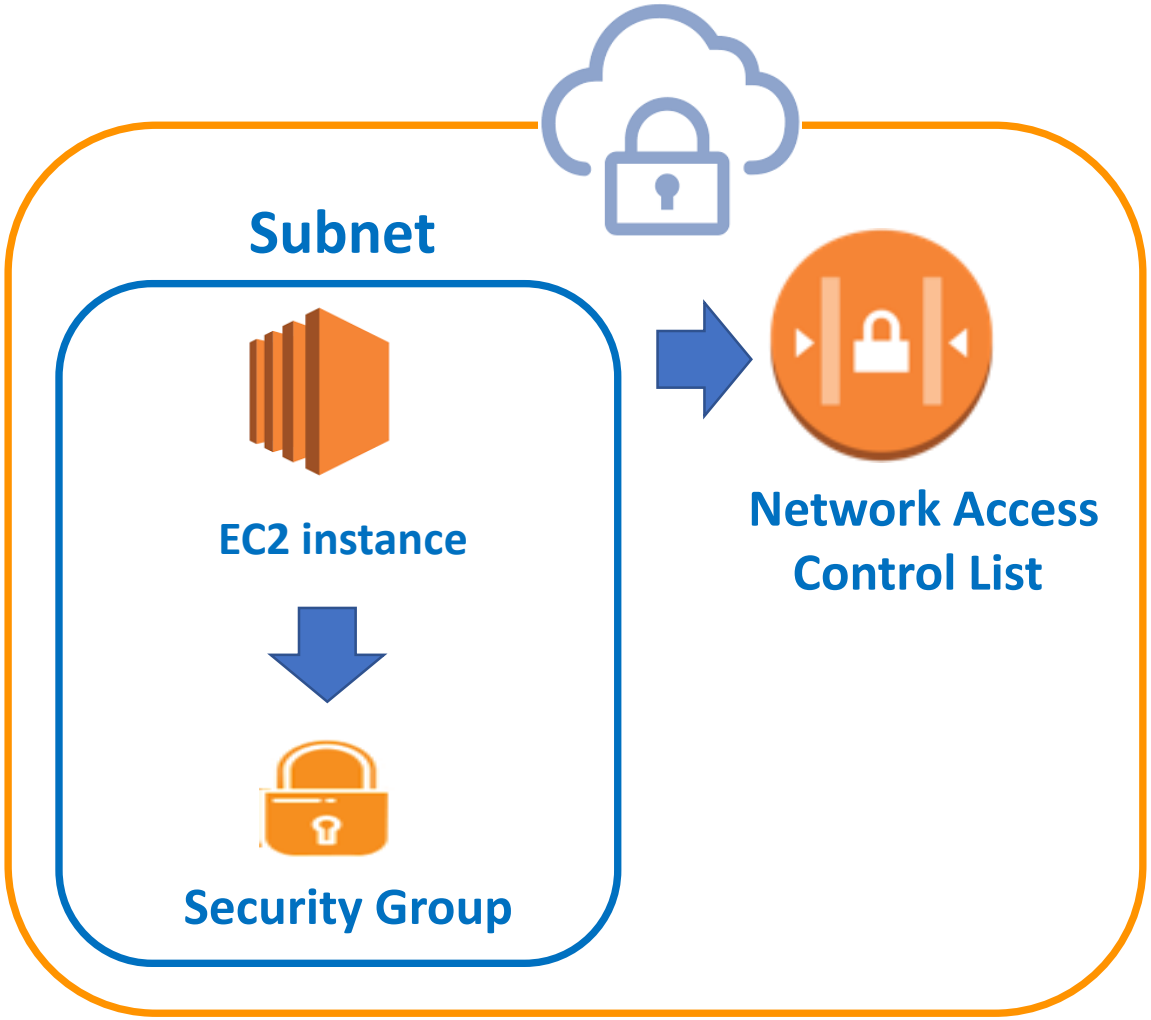
(Network Access List)


Cloud
Region
VPC
10.10.0.0/16
Avaliability Zone 1-a
1
2
3
4
Internet Gateway
10.10.1.0/24
10.10.020/24
10.10.3.0/24
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

Subnet obeys the NACL rules

EC2 obeys NACL and Sec. Group



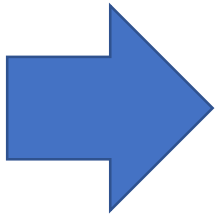
(Statefull) **Security Group inbound**

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**

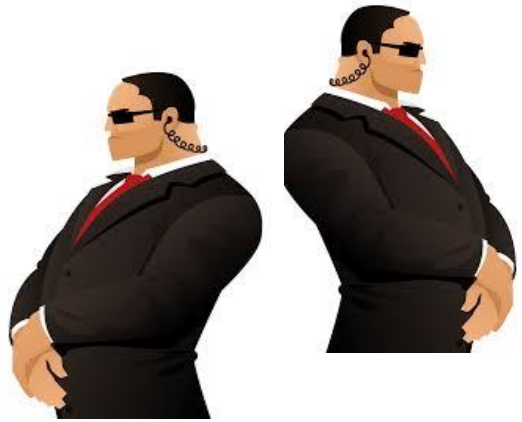
Rule	Type	Protocol	Port Range	Destination	Allow/ Deny
100	HTTP	TCP(6)	80	7.8.9.10/32	ALLOW
200	Custom TCP	TCP(6)	32768 - 65535	0.0.0.0/0	ALLOW
300	All ICMP-IPv4	ICMP(1)	ALL	0.0.0.0/0	ALLOW
400	HTTPS	TCP(6)	443	7.8.9.10/32	DENY
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

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

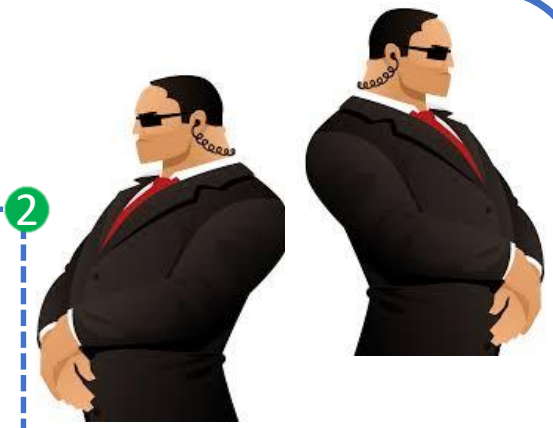
Rule	Type	Protocol	Port Range	Source/ Destination	Allow/ Deny
100	HTTP	TCP(6)	80	7.8.9.10/32	ALLOW
200	SSH-22	TCP(6)	22	0.0.0.0/0	ALLOW
300	All ICMP-IPv4	ICMP(1)	ALL	0.0.0.0/0	ALLOW
400	HTTPS	TCP(6)	443	7.8.9.10/32	DENY
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

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

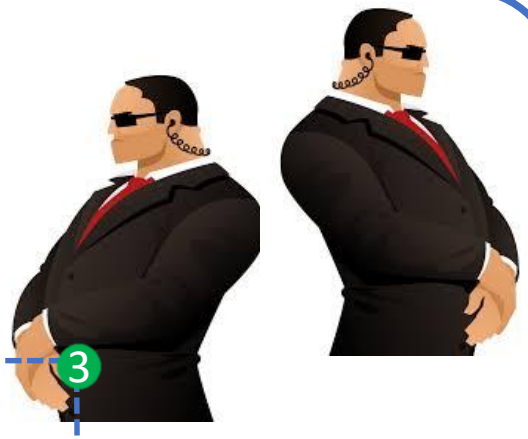
Rule	Type	Protocol	Port Range	Source/ Destination	Allow/ Deny
100	HTTP	TCP(6)	80	7.8.9.10/32	ALLOW
200	SSH-22	TCP(6)	22	0.0.0.0/0	ALLOW
300	All ICMP-IPv4	ICMP(1)	ALL	0.0.0.0/0	ALLOW
400	HTTPS	TCP(6)	443	7.8.9.10/32	DENY
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

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

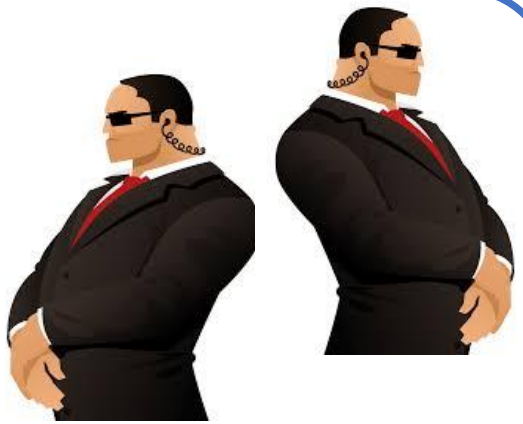
Rule	Type	Protocol	Port Range	Source/ Destination	Allow/ Deny
100	HTTP	TCP(6)	80	7.8.9.10/32	ALLOW
200	SSH-22	TCP(6)	22	0.0.0.0/0	ALLOW
300	All ICMP-IPv4	ICMP(1)	ALL	0.0.0.0/0	ALLOW
400	HTTPS	TCP(6)	443	7.8.9.10/32	DENY
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

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

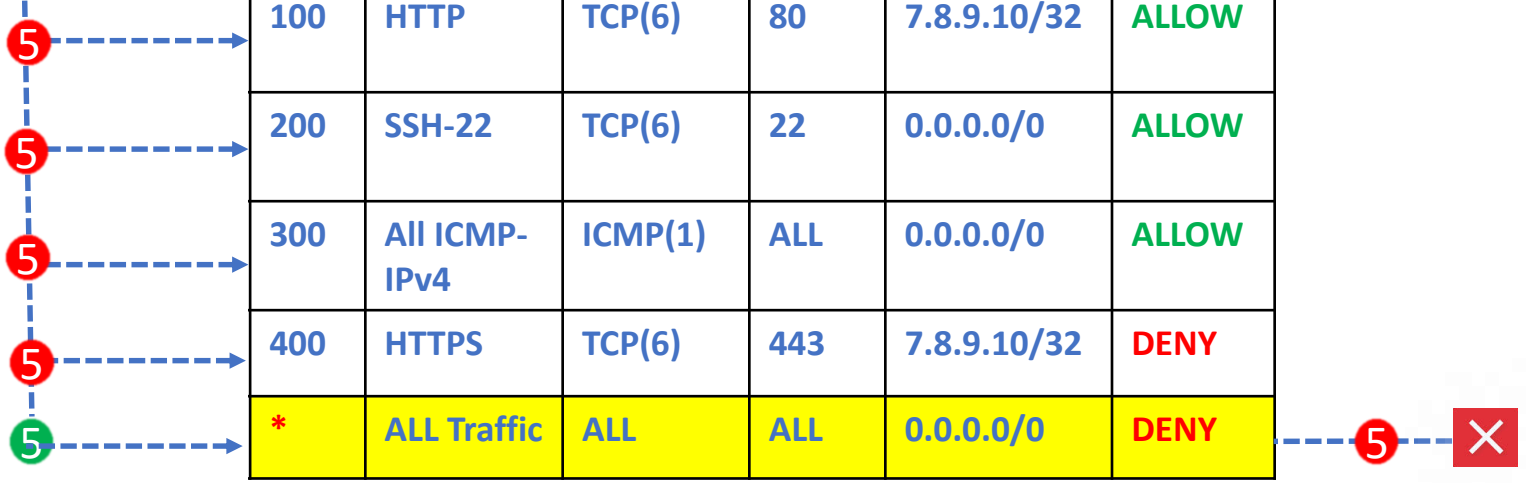
Connection Request	
No	Type-Port
1	SSH-22
2	HTTP-80
3	All ICMP-IPv4 -All
4	HTTPS-443
5	Msql/Auro. 3306

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



2768 -65535

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.

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

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

Subnet