

Amazon VPC-4



Table of Content

- 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



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

us-east-1b

AZ

us-east-1b-Public

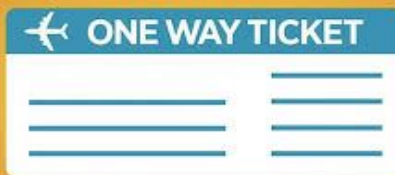
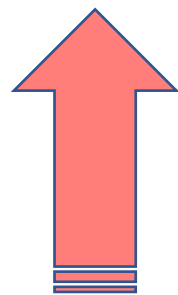
NAT
Instance/EC2

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



?
v
v

User Data



User Data



It is in another instance in the Private Subnet



Cloud

Region



Clarus-VPC-a

1- Desired Scenario



Internet Gateway

Availability Zone 1-a

Availability Zone 1-b

Availability Zone 1-c

Public Subnet 1a



Private Subnet 1a

Public Subnet 1b



Private Subnet 1b

Public Subnet 1c



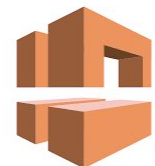
Private Subnet 1c



Cloud



Region

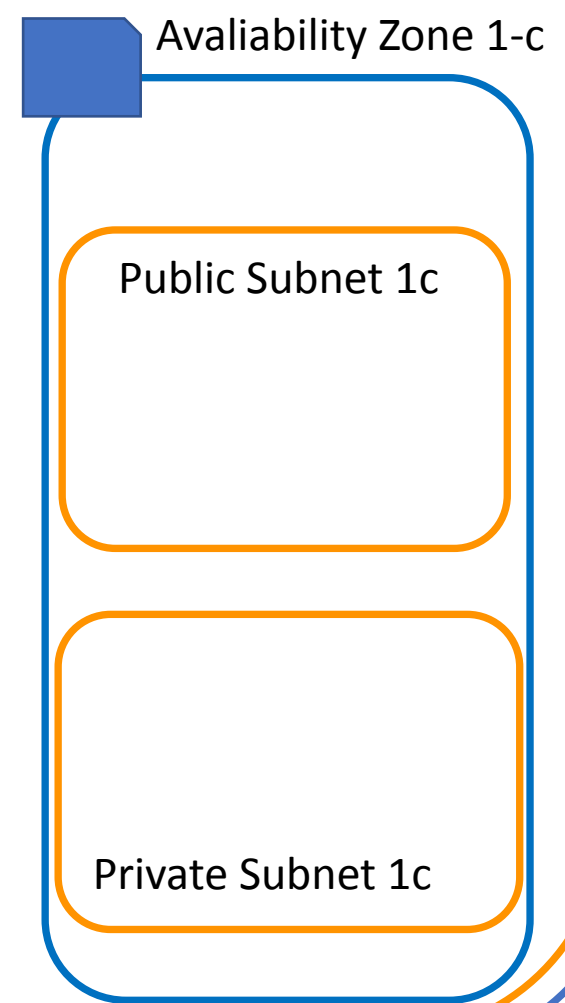
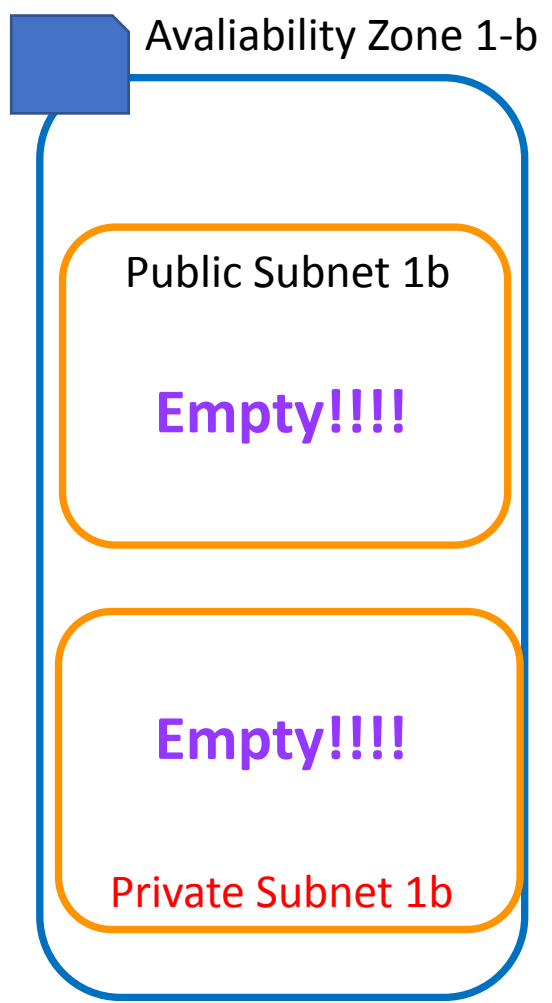
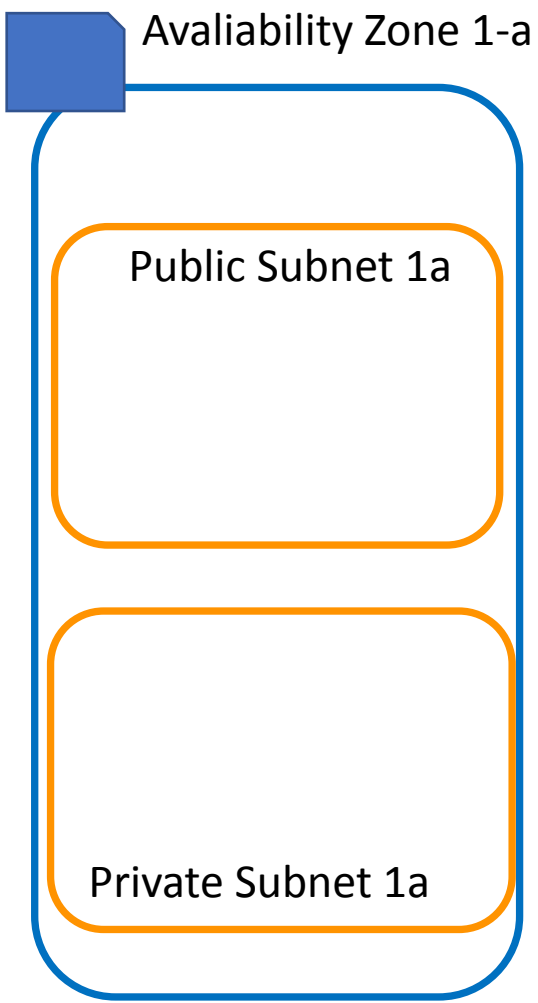


VPC

2- Where we are



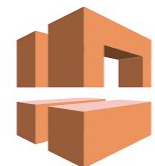
Internet Gateway





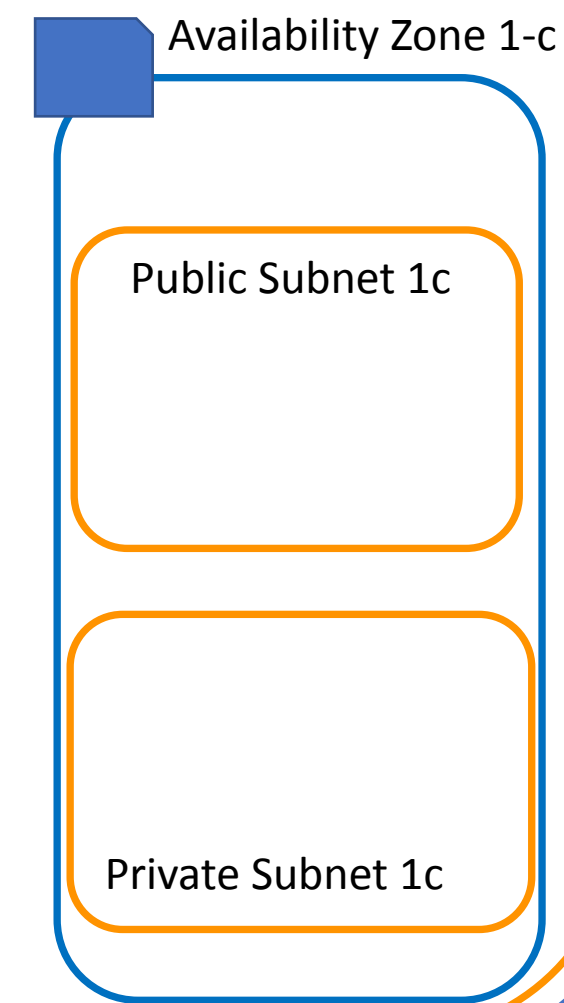
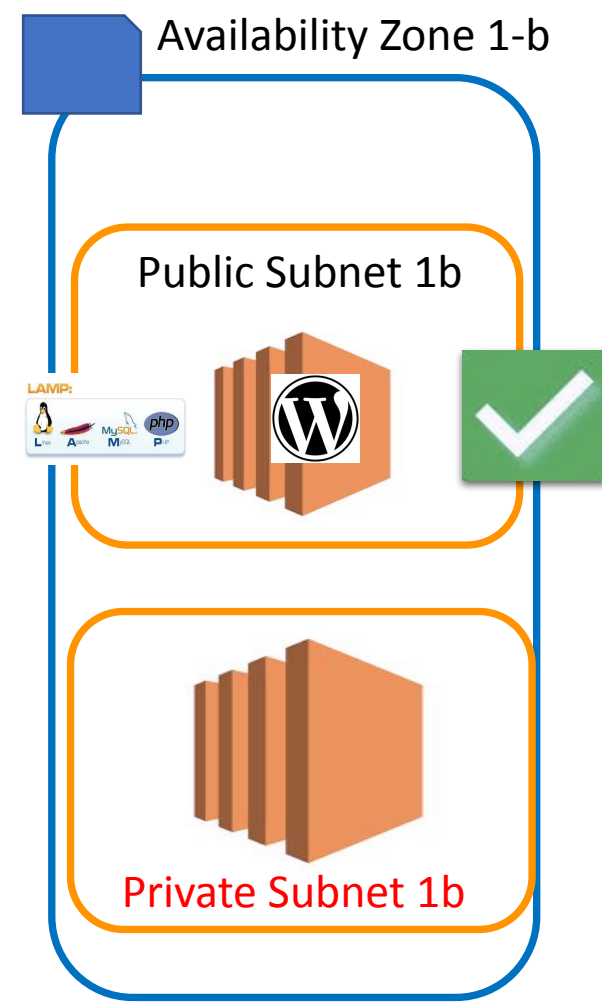
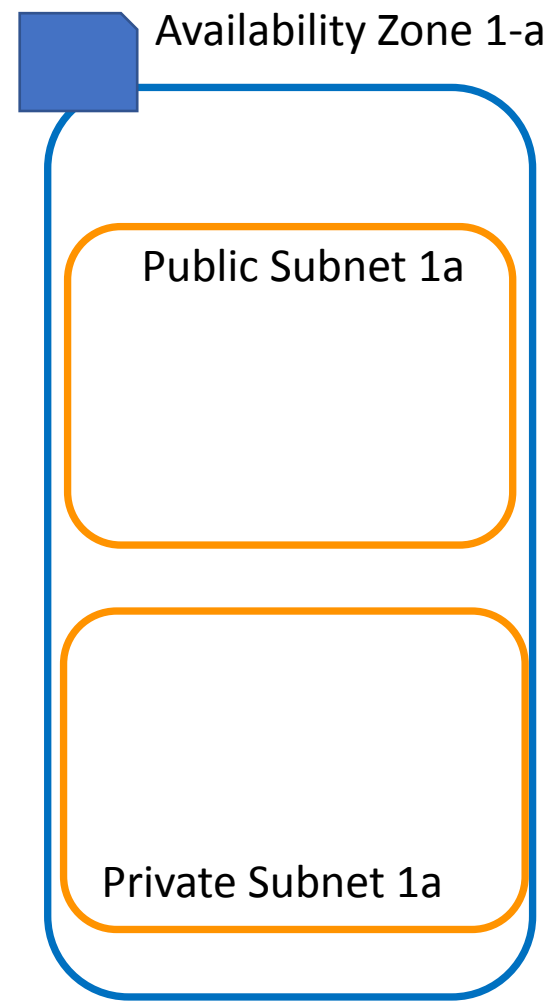
Cloud

Region



VPC

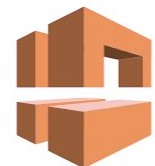
3- Wordpress Instance is ready what about DB





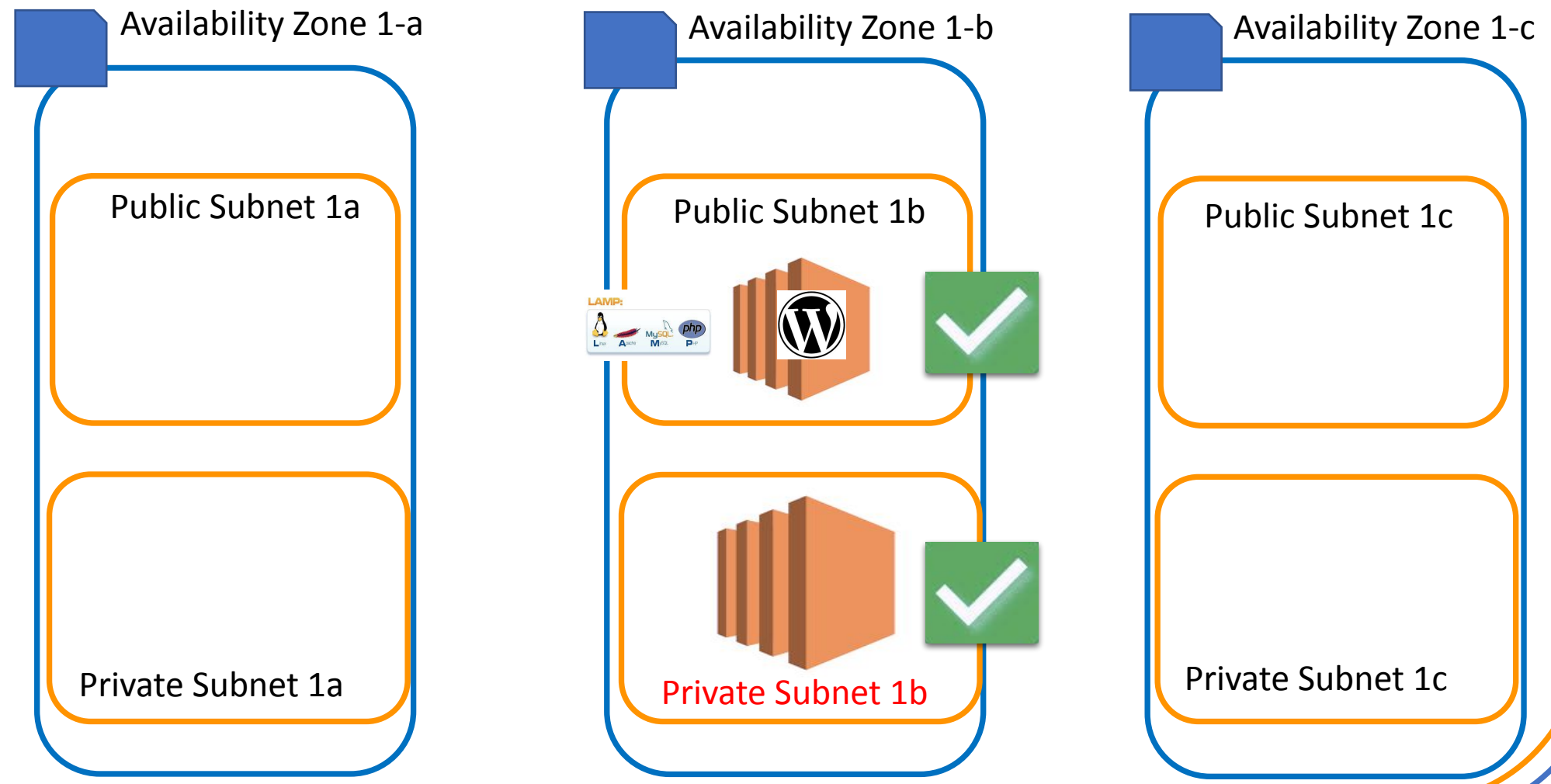
Cloud

Region



VPC

3- Wordpress Instance and Database are ready




Security Group Best Practice

Bastion Host

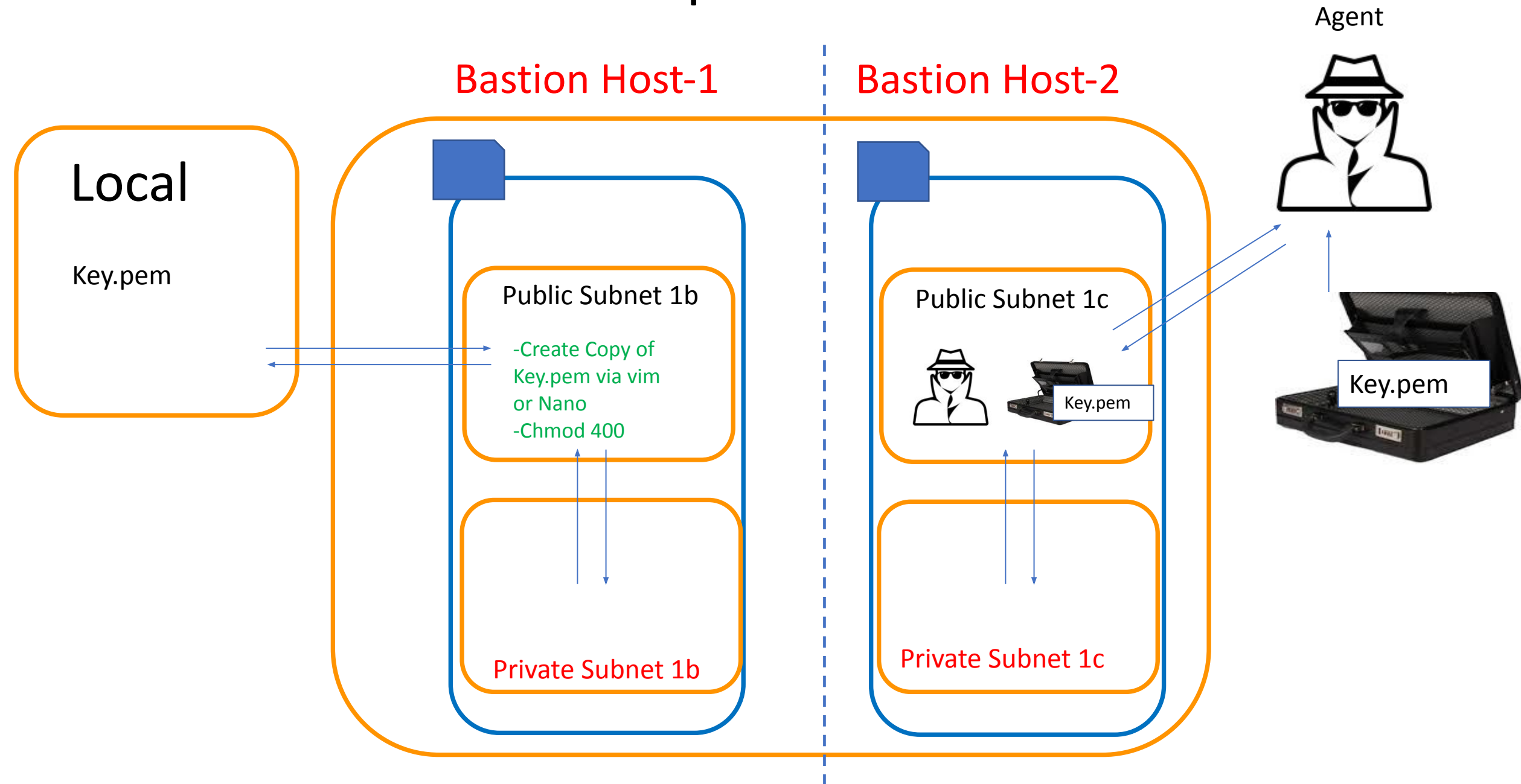
Inbound rules [Info](#)

Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info	
All traffic ▼	All	All	Custom ▼	<input type="text"/>	<input type="button" value="Delete"/>



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

.pem Issue



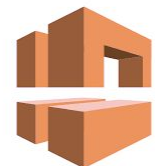


Cloud



Internet Gateway

Region



VPC

3- You are here now

Availability Zone 1-a

Availability Zone 1-b

Availability Zone 1-c

Public Subnet 1a

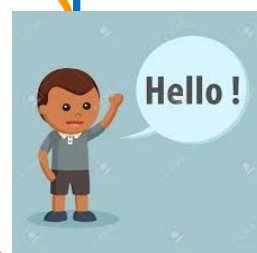
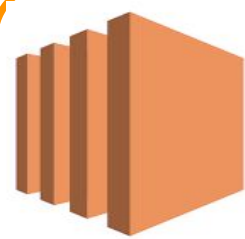
Public Subnet 1b

Public Subnet 1c

Private Subnet 1a

Private Subnet 1b

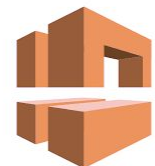
Private Subnet 1c





Cloud

Region



VPC



Internet Gateway

3- Try to install mariaDB



Public Subnet 1a

Private Subnet 1a



Public Subnet 1b



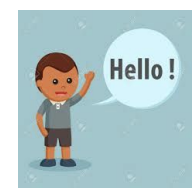
Private Subnet 1b

1

Bastion Host

2

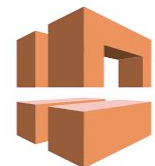
Install mariadb





Cloud

Region

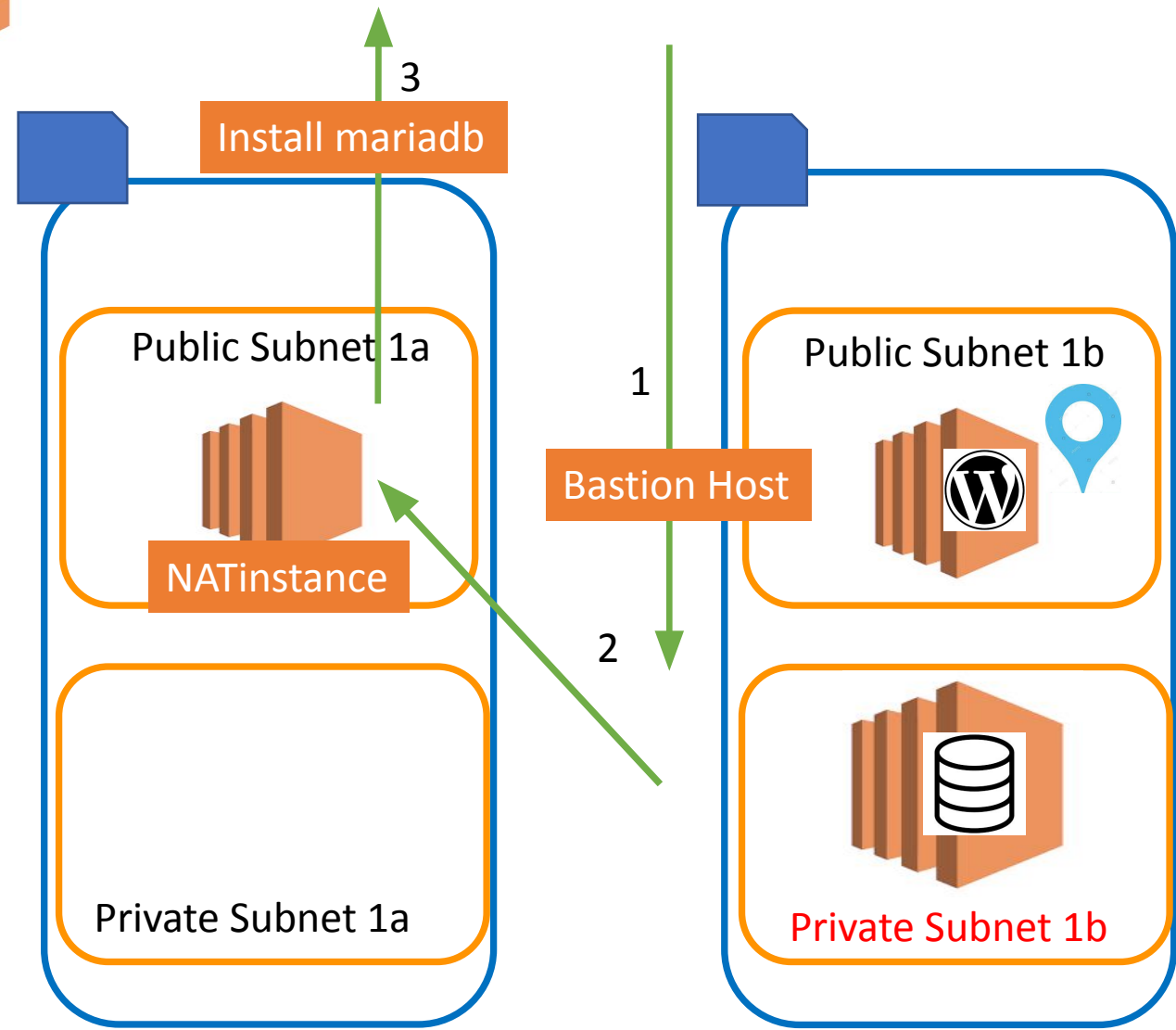


VPC



Internet Gateway

4- Try NAT instance



NAT INSTANCE

[Route Tables](#) > Edit routes

Edit routes

1- Route table Issue

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

Add route



- Nat Gateway



Cloud



Region

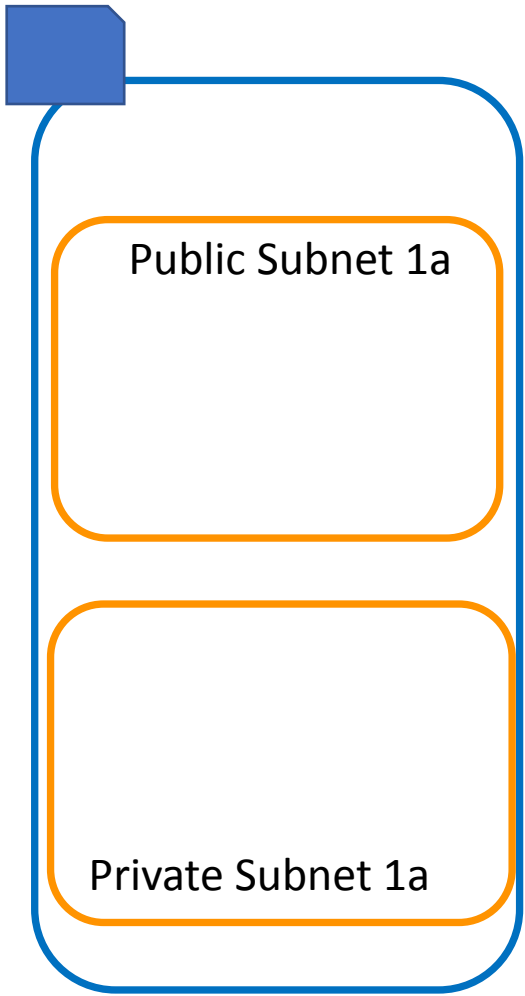


VPC



Internet Gateway

5- Associate DATABASE

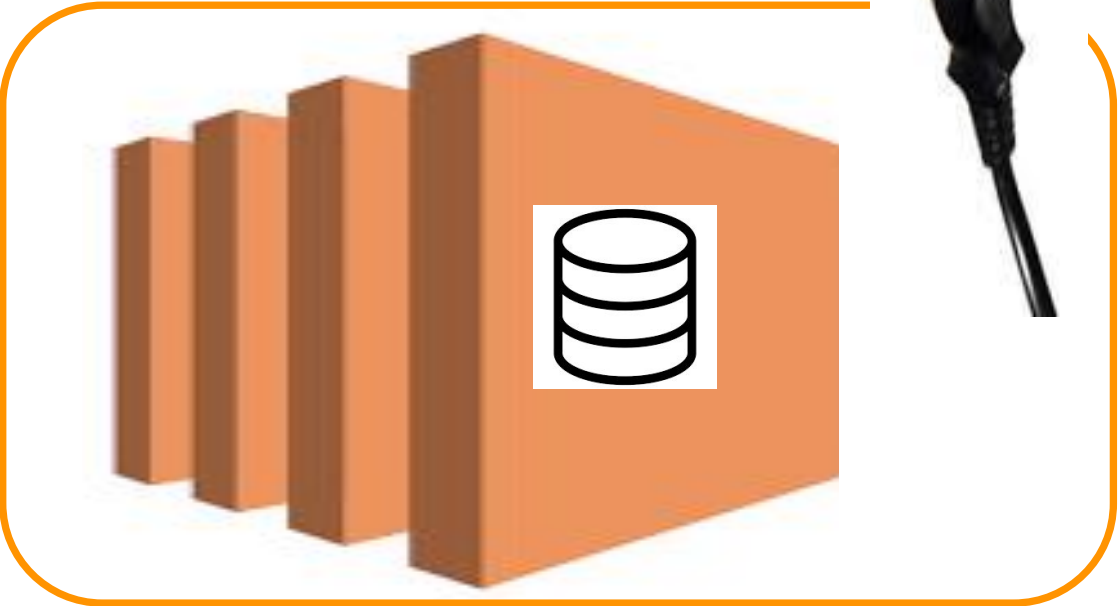


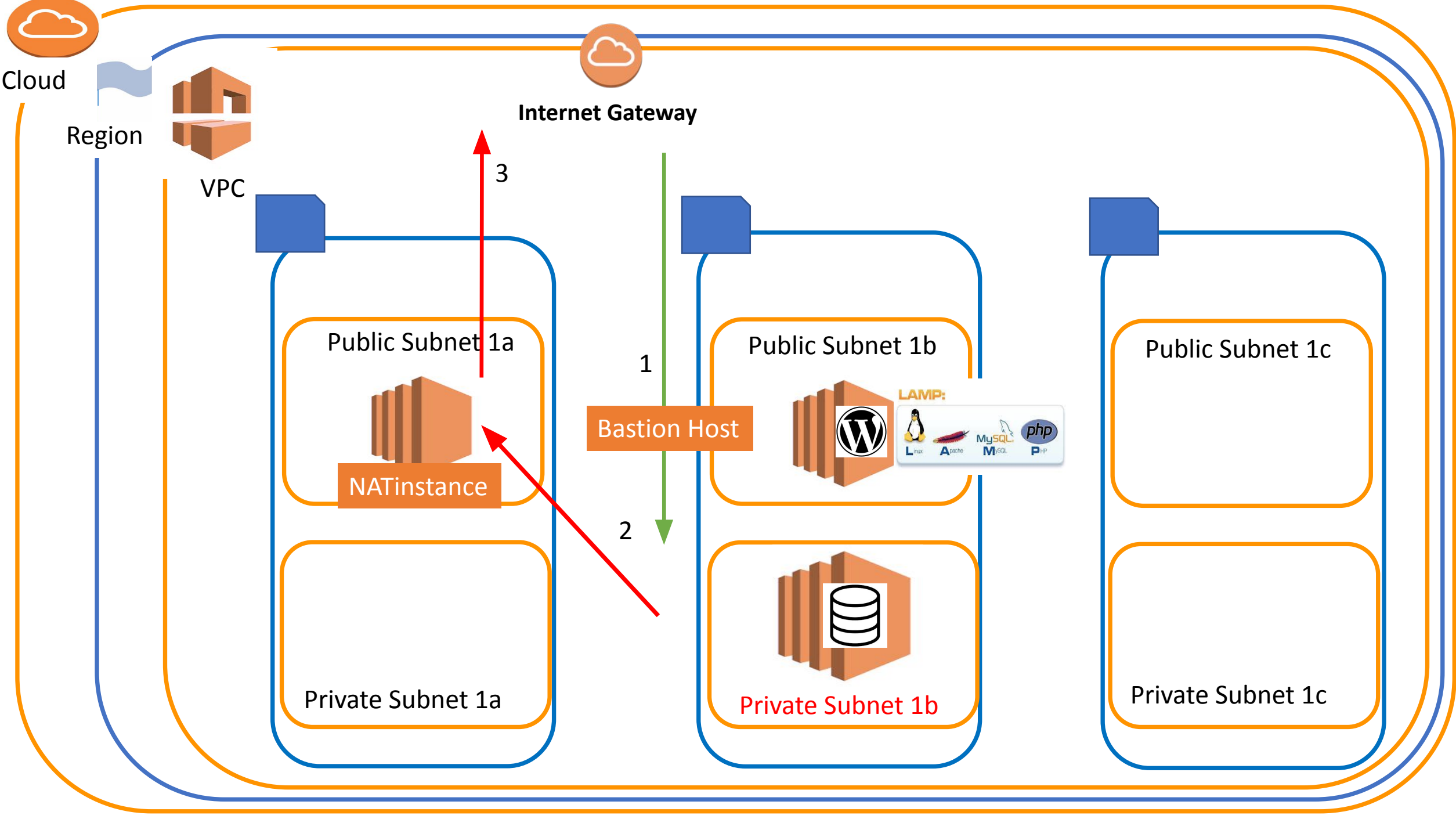
Associate DATABASE

Public Subnet 1b



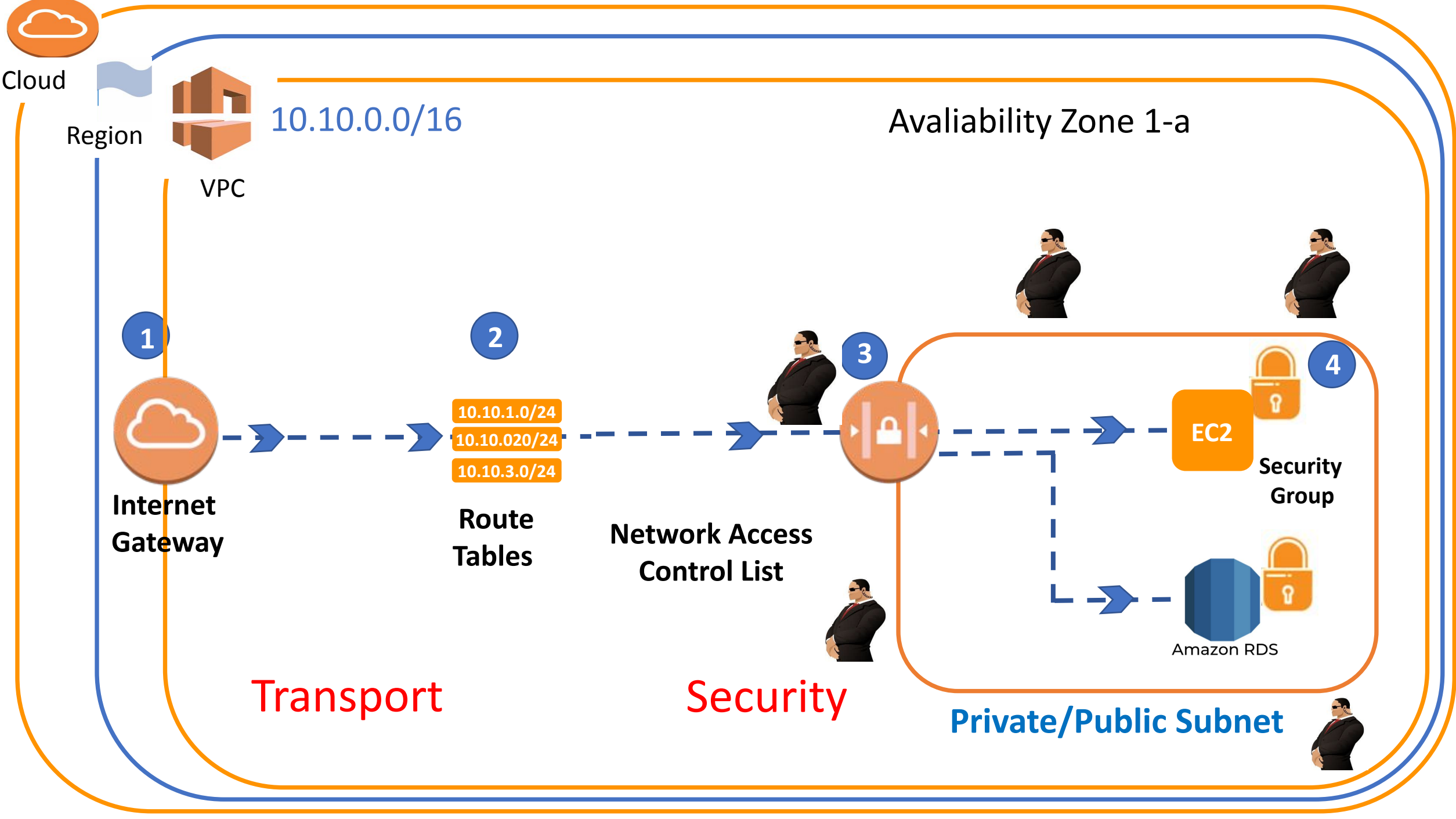
Private Subnet 1b

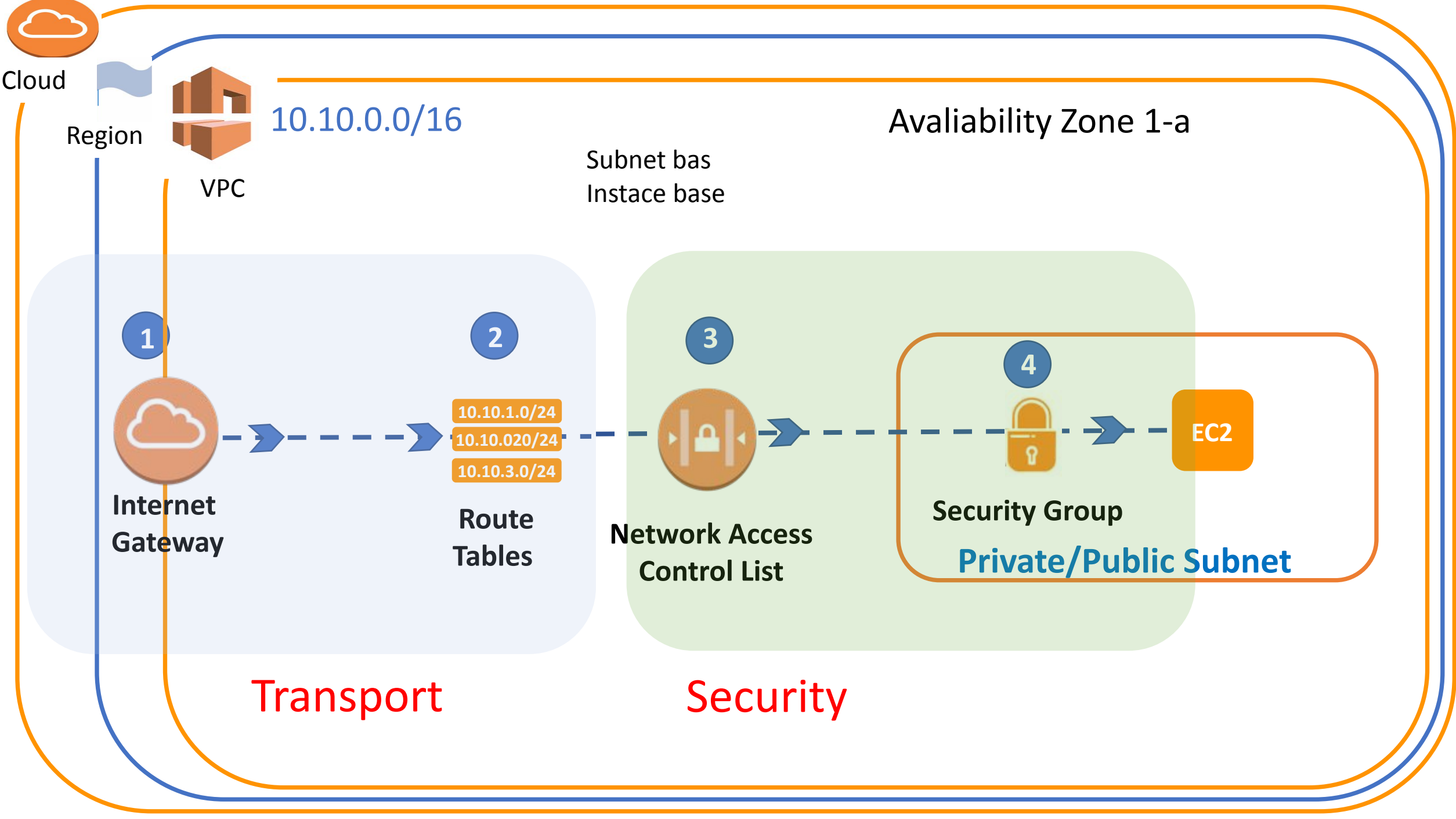






NACL (NETWORK ACCESS LISTS)

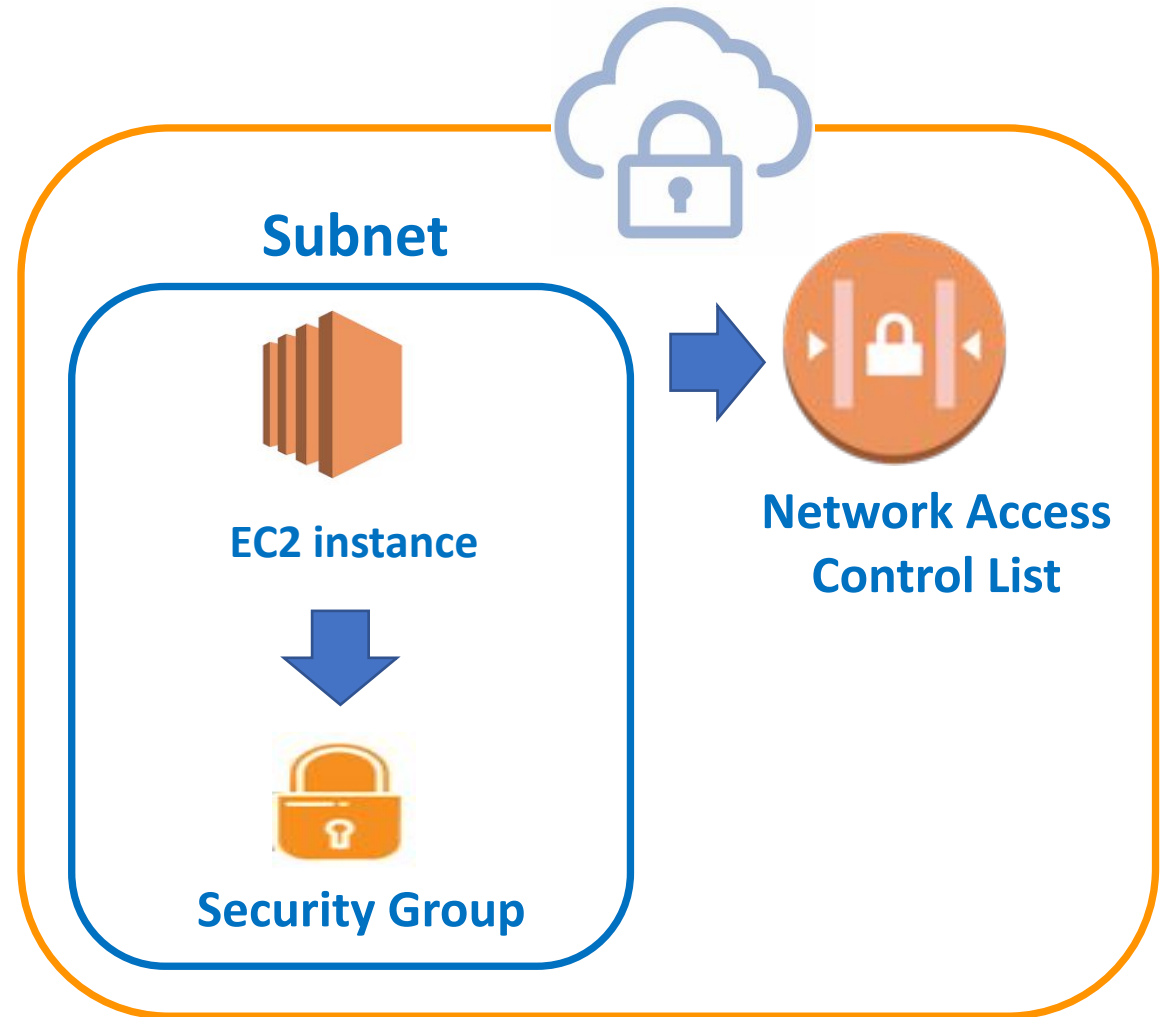




NACL (NETWORK ACCESS LISTS)

Subnet obeys the **NACL** rules

Resources obeys **NACL** and **Sec. Group**



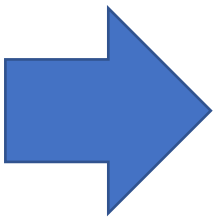
(Statefull) **Security Group inbound**

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:

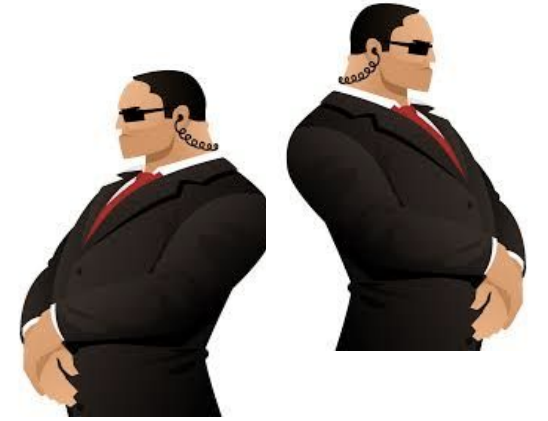
Connection Request

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 inbound

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 inbound

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

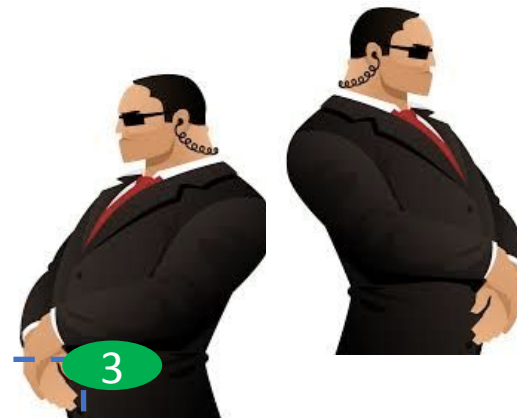


Security Group inbound

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



3



3

Network ACL inbound

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

3

3

3



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 inbound

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

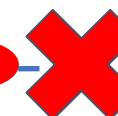
4

4

4

4

4





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	Mysql/Auro. 3306



EC2

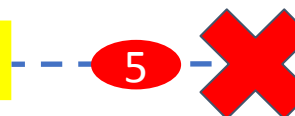
Security Group inbound

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 inbound

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



THANKS!

Any questions?

Instructor: @serdar-instructor

Email: serdar@clarusway.com



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