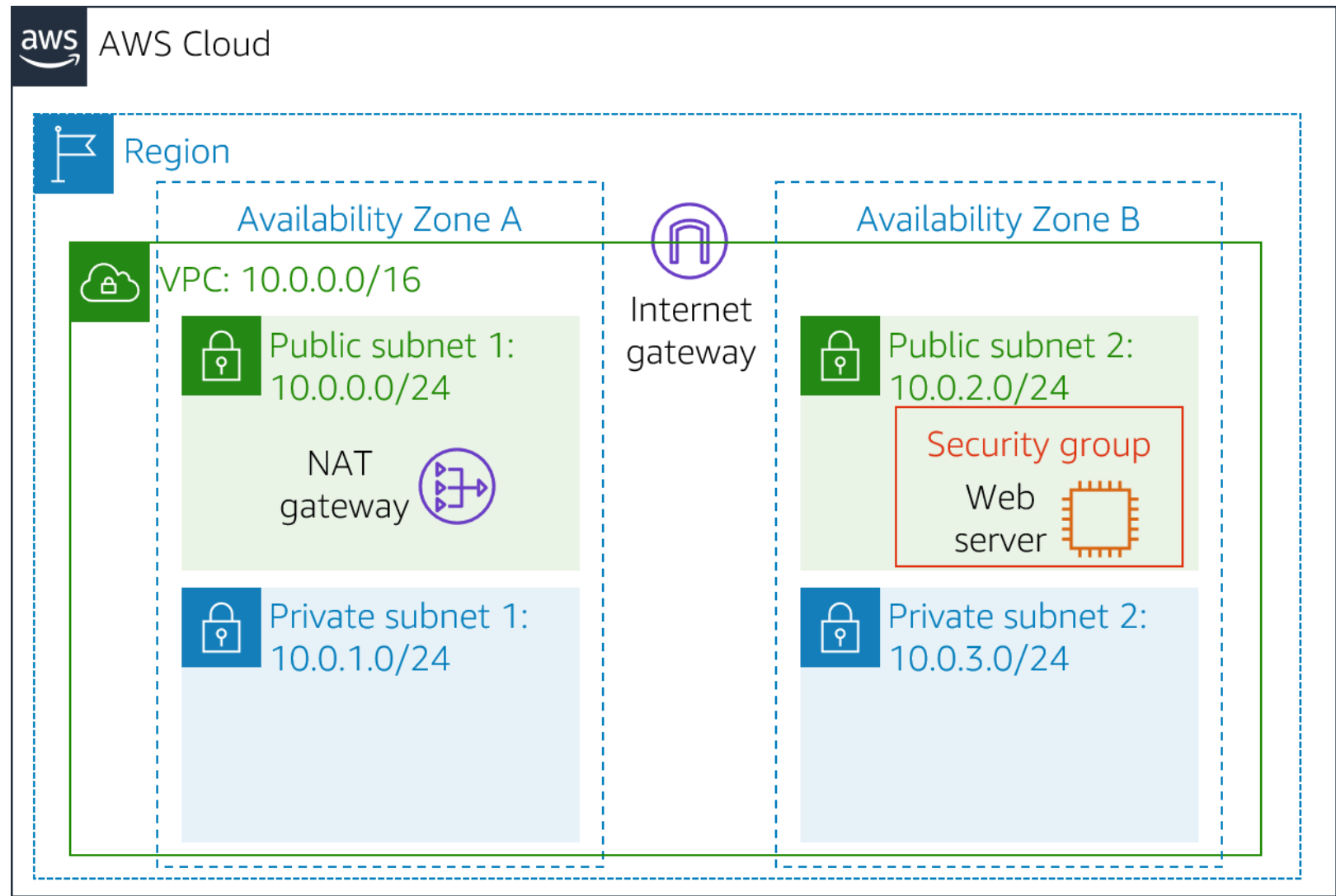


Lab 2: Build your VPC and Launch a Web Server



สำหรับ public subnet 1&2

Public Route Table

Destination	Target
10.0.0.0/16	Local
0.0.0.0/0	Internet gateway

สำหรับ private subnet 1&2

Private Route Table

Destination	Target
10.0.0.0/16	Local
0.0.0.0/0	NAT gateway

Region

ใน cloud จะแบ่งเป็น region ว่าฮาร์ดแวร์จริงอยู่ที่ใด เช่น US East, US West, ... แยกไปตามแต่ละทวีปทั่วโลก แต่ละ region แบ่งเป็น Availability Zone เช่น US East แบ่งเป็น

us-east-1 (N. Virginia), us-east-2 (Ohio)

ควรมีทรัพยากรอยู่บน 2 availability zone ที่อยู่คนละสถานที่กัน

เพื่อว่าที่หนึ่งมันใช้งานไม่ได้ จะได้เหลืออีกที่หนึ่งใช้งานได้

us-east-1 ยังแยกเป็น 1a, 1b, 1c, 1d, 1e, 1f

VPC = Virtual Private Cloud ก็คือ network ส่วนตัว (ลับ) คนอื่น ๆ บนอินเทอร์เน็ตมองไม่เห็น network นี้

อยู่ต่าง zone (สถานที่) กัน แต่ "virtual network" เชื่อมให้เป็น network เดียวกันได้ เป็น VPC ขึ้นเดียว

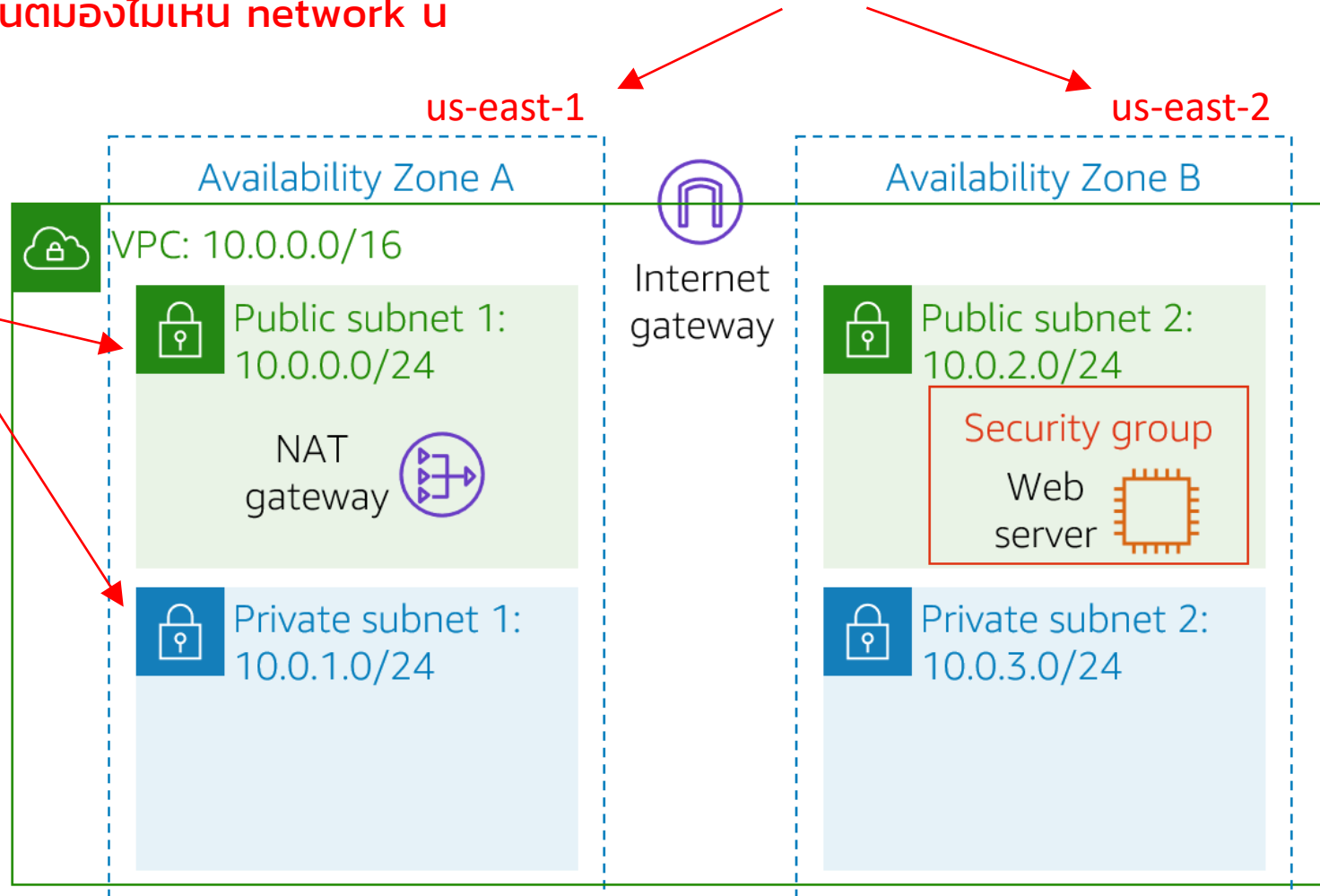
ใน zone แบ่งเป็น public และ private network

Public subnet

vm บนนี้ส่ง traffic ออกไปบนอินเทอร์เน็ตได้เลย vm ที่ควรอยู่ที่นี่ เช่น web server รับ request จากอินเทอร์เน็ตได้ และส่งข้อมูลกลับไปให้ผู้เยี่ยมชมเว็บไซต์โดยตรง

Private subnet

vm บนนี้ส่ง traffic ออกไปบนอินเทอร์เน็ตโดยตรงไม่ได้ vm ที่ควรอยู่ที่นี่ เช่น database server รับ request จากอินเทอร์เน็ตไม่ได้ และถ้าจะส่งข้อมูลออกไป เช่น อัปเดตซอฟต์แวร์เวอร์ชันใหม่ ต้องผ่าน NAT



request เช่น มีคอมพิวเตอร์บนอินเทอร์เน็ตขอใช้บริการ web / ftp เป็นต้น
vm = virtual machine บน cloud นับหน่วยเป็น instance

Subnet



Public subnet 1:
10.0.0.0/24

IP address เริ่มต้นด้วย

10.0.**0**.x



Public subnet 2:
10.0.2.0/24

IP address เริ่มต้นด้วย

10.0.**2**.x



Private subnet 1:
10.0.1.0/24

IP address เริ่มต้นด้วย

10.0.**1**.x



Private subnet 2:
10.0.3.0/24

IP address เริ่มต้นด้วย

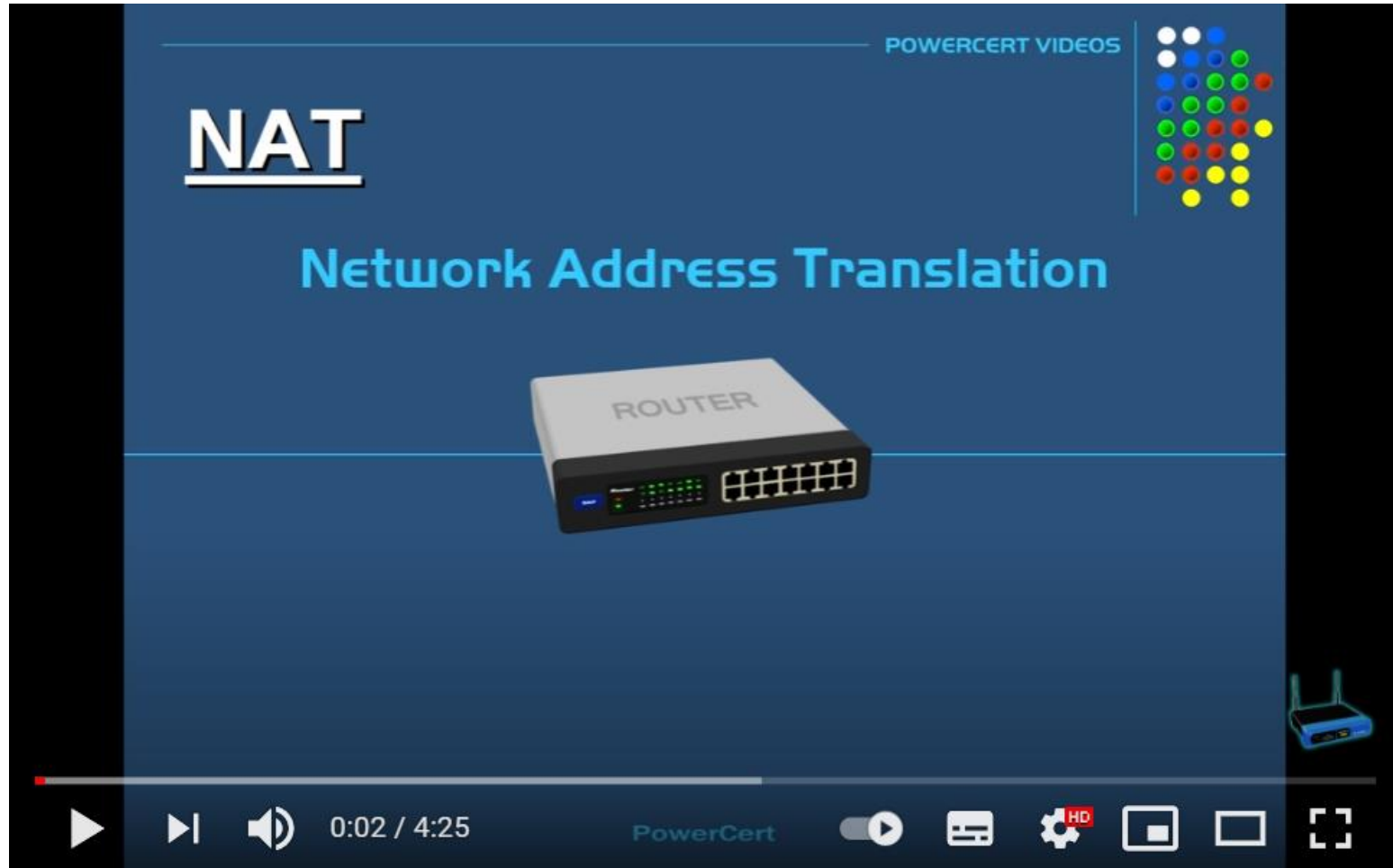
10.0.**3**.x

x.x.x.x/24 หมายถึง 24 บิตข้างหน้า IP address เป็น prefix (x ตัวละ 8 บิต)
ใน public subset 1 จะมี IP address จาก 10.0.0.0 – 10.0.0.255 ($2^8 = 256$ หมายเลข)

ใช้ได้จริงแค่ 251 หมายเลข AWS จอง 0, 1, 2, 3, 255 ไว้ใช้เอง (reserved)

Network Address Translation (NAT)

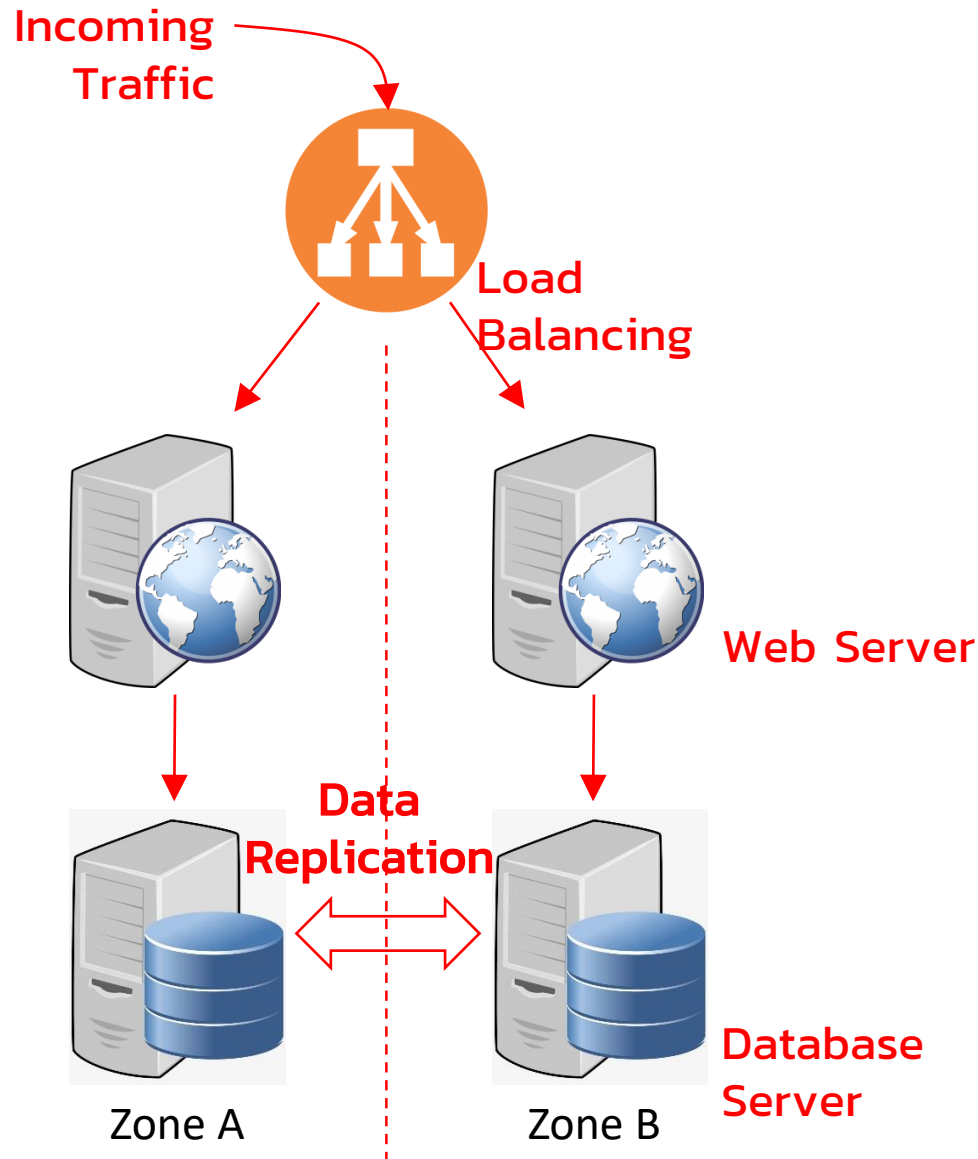
Assume ว่านิสิตรู้จัก IP address และมีความรู้พื้นฐานเกี่ยวกับอินเทอร์เน็ตมาบ้างแล้ว
สาเหตุที่ต้องใช้ NAT เพราะ vm บน VPC ใช้ private IP address



<https://www.youtube.com/watch?v=FTUV0t6JaDA>

High Availability (HA)

จะใช้ cloud หรือ
ซื้ออุปกรณ์ฮาร์ดแวร์มาทำเองก็ได้



Zone A และ Zone B มีระบบไฟฟ้าและ
เครือข่ายแยกเป็นอิสระจากกัน

ถ้า zone ใดเสีย จะเหลืออีก zone ยังให้
บริการได้จึงเรียกว่า **High Availability**
หรือ HA

การทำ replication หมายถึง ถ้ามีการเขียน
database ตัวใดตัวหนึ่ง ให้เขียน database อีกตัว
หนึ่งด้วย เพื่อ sync ข้อมูลให้ตรงกัน

Zone ที่อยู่บน region เดียวกันเชื่อมกันด้วย high-
speed network ที่เร็วมาก จึงทำ data replication
ได้

us-east-1a

Step 2: VPC with Public and Private Subnets

IPv4 CIDR block:* (65531 IP addresses available)

IPv6 CIDR block: ☒ No IPv6 CIDR Block
☐ Amazon provided IPv6 CIDR block
☐ IPv6 CIDR block owned by me

VPC name:

Public subnet's IPv4 CIDR:* (251 IP addresses available)

Availability Zone:*

Public subnet name:

Private subnet's IPv4 CIDR:* (251 IP addresses available)

Availability Zone:*

Private subnet name:

You can add more subnets after Amazon Web Services creates the VPC.

Specify the details of your NAT gateway ([NAT gateway rates apply](#)).

Elastic IP Allocation ID:*

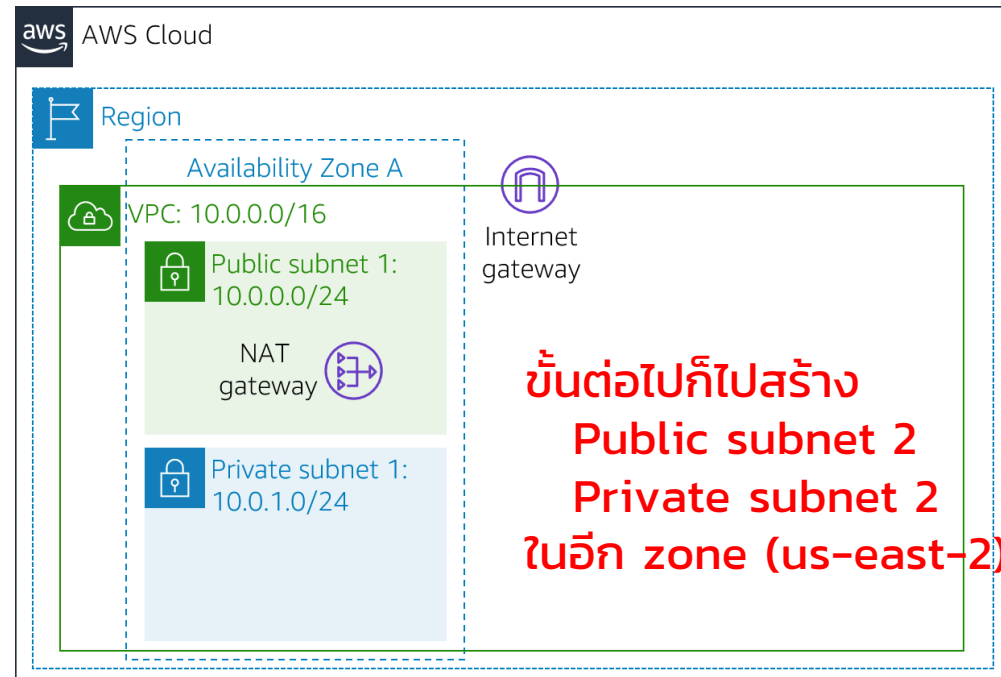
Service endpoints	Allocation ID	Elastic IP Address
	eipalloc-05fd8d98531a657bf	44.197.69.66

Enable DNS hostnames:* ☒ Yes ☐ No

Hardware tenancy:*

Public IP ของ NAT

จะได้
Public/Private
route table



ขั้นตอนต่อไปสร้าง
Public subnet 2
Private subnet 2
ในอีก zone (us-east-2)

Public Route Table

Destination	Target
10.0.0.0/16	Local
0.0.0.0/0	Internet gateway

Private Route Table

Destination	Target
10.0.0.0/16	Local
0.0.0.0/0	NAT gateway

Destination Target Main=No

10.0.0.0/16	local	
0.0.0.0/0	igw-03d4d3b021c7be115	

ต้องเอาไป associate กับ
Public subnet 1 และ 2

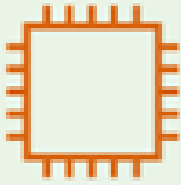
Destination Target Main=Yes

10.0.0.0/16	local	
0.0.0.0/0	nat-03cd5573ee14bc7dd	

ต้องเอาไป associate กับ
Private subnet 1 และ 2

Security group

Web
server



Inbound rules [Info](#)

Security group rule ID

Type [Info](#)

Protocol
[Info](#)

Port range
[Info](#)

Source [Info](#)

sgr-005d4c4d60503a55d

HTTP ▼

TCP

80

Anywh... ▼

อนุญาตให้ traffic เข้าที่เป็น protocol แบบ HTTP (port 80) ที่มาจาก source (IP addr) ใดก็ได้

All services



Compute

EC2

Lightsail

Lambda

Batch

Elastic Beanstalk



Amazon Linux

Free tier eligible

Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-

0c2b8ca1dad447f8a (64-bit x86) / ami-06cf15d6d096df5d2 (64-bit Arm)

Amazon Linux 2 comes with five years support. It provides Linux kernel 4.14 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras. This AMI is the successor of the Amazon Linux AMI that is approaching end of life on December 31, 2020 and has been removed from this wizard.

Root device type: ebs

Virtualization type: hvm

ENA Enabled: Yes

Select

☒ 64-bit (x86)

☐ 64-bit (Arm)

Launch instances

Filter by:

t2

Current generation

Show/Hide Columns

Currently selected: t2.micro (- ECUs, 1 vCPUs, 2.5 GHz, -, 1 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)
☐	t2	t2.nano	1	0.5	EBS only
☒	t2	t2.micro Free tier eligible	1	1	EBS only
☐	t2	t2.small	1	2	EBS only

Number of instances	1	Launch into Auto Scaling Group
Purchasing option	☐ Request Spot instances	
Network	vpc-061ae9e6e9d1e5169 Lab VPC	Create new VPC
Subnet	subnet-016a3f8aaad591cec Public Subnet 2 us-ea 251 IP Addresses available	Create new subnet
Auto-assign Public IP	Enable	
Placement group	☐ Add instance to placement group	
Capacity Reservation	Open	
Domain join directory	No directory	Create new directory
IAM role	None	Create new IAM role
Shutdown behavior	Stop	
Stop - Hibernate behavior	☐ Enable hibernation as an additional stop behavior	
Enable termination protection	☐ Protect against accidental termination	

▼ Advanced Details

Enclave	☐ Enable
Metadata accessible	Enabled
Metadata version	V1 and V2 (token optional)
Metadata token response hop limit	1
User data	☒ As text ☐ As file ☐ Input is already base64 encoded

```
#!/bin/bash
# Install Apache Web Server and PHP
yum install -y httpd mysql php
# Download Lab files
wget https://aws-tc-largeobjects.s3.us-west-2.amazonaws.com/CUR-TF-100-ACCLFO-2/2-lab2-vpc/s3/lab-app.zip
```

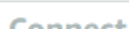
ตอนติดตั้ง OS ให้ติดตั้งโปรแกรม web server
และใส่ข้อมูล web site ลงไปด้วย

เป็นคำสั่งที่ใช้ติดตั้งโปรแกรม web server
และดาวน์โหลด web site มาติดตั้ง

เป็นคำสั่งของ Amazon Linux
(distro พิเศษสำหรับ AWS Cloud)
คำสั่งจะไม่เหมือนของ Ubuntu Linux

```
#!/bin/bash
# Install Apache Web Server and PHP
yum install -y httpd mysql php
# Download Lab files
wget https://aws-tc-largeobjects.s3.us-west-2.amazonaws.com/CUR-TF-100-ACCLFO-2/2-lab2-vpc/s3/lab-app.zip
unzip lab-app.zip -d /var/www/html/
# Turn on web server
chkconfig httpd on
service httpd start
```

Instances (2) [Info](#)

Instance state ▼

Actions ▼

Launch

 Filter instances

☐	Name ▼	Instance ID	Instance state ▼	Instance type ▼	Status check	Alarm status	Availability Zone
☐	Bastion Host	i-00182d27095272af2	 Running  	t2.micro	 2/2 checks passed	No alarms +	us-east-1a
☐	Web Server 1	i-00bdded894d4e2ed6	 Pending  	t2.micro	–	No alarms +	us-east-1b

Instances (2) [Info](#)



Connect

Instance state ▼

Actions ▼

Launch



Filter instances

☐	Name ▼	Instance ID	Instance state ▼	Instance type ▼	Status check	Alarm status	Availability Zone
☐	Bastion Host	i-00182d27095272af2	 Running  	t2.micro	 2/2 checks passed	No alarms 	us-east-1a
☐	Web Server 1	i-00bdded894d4e2ed6	 Running  	t2.micro	 Initializing	No alarms 	us-east-1b

Instances (2) [Info](#)

คลิกที่นี่ 

ต้อง checks passed ก่อน ถึงจะเริ่มใช้งานได้

Instance summary for i-00bddd894d4e2ed6 (Web Server 1)

[Info](#)

Updated less than a minute ago



Connect

Instance state ▼

Actions ▼

Instance ID

i-00bddd894d4e2ed6 (Web Server 1)

Private IPv4 addresses

10.0.2.220

Instance state

Running

Private IPv4 DNS

ip-10-0-2-220.ec2.internal

Elastic IP addresses

—

Public IPv4 address

18.212.185.209 [open address](#)

IPv6 address

—

Public IPv4 DNS

ec2-18-212-185-209.compute-1.amazonaws.com | [open address](#)

Instance type

t2.micro

VPC ID

vpc-061ae9e6e9d1e5169 (Lab VPC)

คลิกเปิดเว็บไซต์บน **browser (new tab)**
จะเปิดไม่ได้เพราะเป็น **https**

⚠️ ไม่ปลอดภัย | 18.212.185.209 ต้องใช้ **http** ใช้ **https** ไม่ได้ เพราะเรายังไม่ได้ติดตั้ง **https**

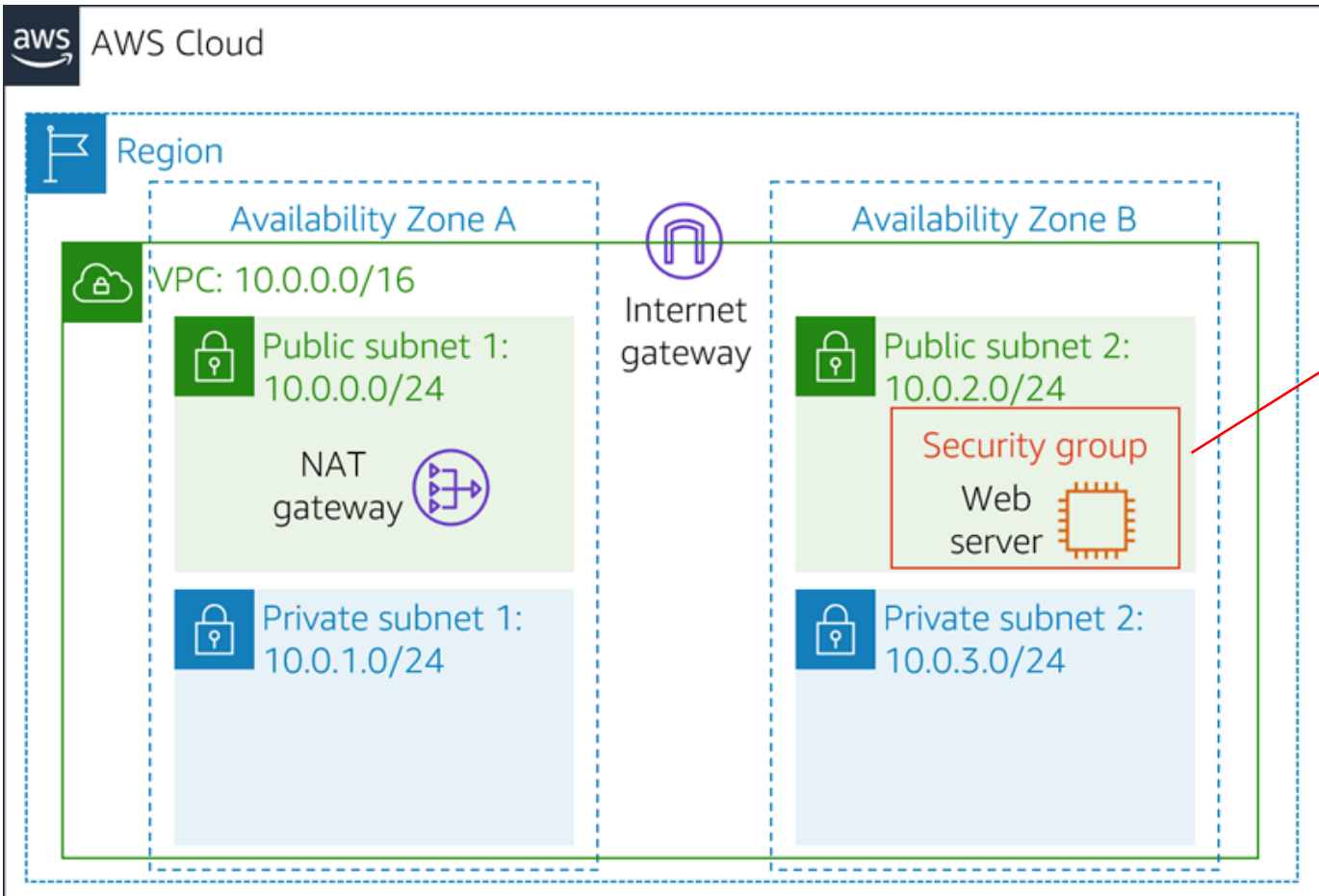


Load Test

RDS

Meta-Data	Value
InstanceId	<i>i-00bdded894d4e2ed6</i>
Availability Zone	<i>us-east-1b</i>

Current CPU Load: **0%**



- Instance ที่สร้างขึ้นกำหนดให้มีทั้ง 2 IP addr
- Public IP เช่น a.b.c.d จึงเอา IP นี้ไปเปิดบน web browser ได้
 - Private IP (10.0.2.x)

ระบบจะสุ่มแจก IP ให้โดยอัตโนมัติทั้ง public และ private IP

เมื่อ shutdown และ boot instance นี้ใหม่ ก็จะได้ IP ใหม่

ต้องจ่ายเงินซื้อ static IP ถึงจะไม่เปลี่ยนเวลา boot ใหม่

จ่ายเงินจดโดเมนเนมได้ เช่น abc.com ให้ชี้มาที่ public IP นี้